Task Order ID: ID04140199 **Awarded: 30 March 2015** Mod 01: 28 May 2015 Mod 02: 30 Mar 2016 Mod 03: 14 June 2016 Mod 04: 24 January 2017 Mod 05: 2 February 2018 Mod 06: 25 August 2018 Mod 07: 20 September 2018 Mod 08: 5 February 2018 Mod 09: 27 August 2018 Mod 10: 9 January 2018 Mod 11: 11 March 2019 Mod 12: 12 March 2019	**GSA Customer Accounts Manager (CAM):** Ronald P Alexander Phone: (b) (6) Email: ronald.alexander@gsa.gov General Services Administration FAS/AASD/Branch B 401 West Peachtree Street Atlanta, GA 30308 **GSA Senior Contracting Officer:** Rodney C. Lewis Phone: (b) (6) Email: rodney.lewis@gsa.gov
Client Organization: USAFCENT A6 Network Operations and Security Center (NOSC)	**COR / Client Representative:** Keren Preston Phone: (b) (6) USAFCENT A6O Shaw AFB, SC 29152 Email: keren.preston@nosc.afcent.af.mil
Project Name: HQ USAFCENT A6 NOSC IT Professional Services	**Period of Performance** Base Year - 4/1/2015 thru 3/31/2016 Option Year 1 - 4/1/2016 thru 3/31/2017 Option Year 2 - 4/1/2017 thru 3/31/2018 Option Year 3 – 4/1/2018 thru 3/31/2019 **Option Year 4 – 4/1/2019 thru 3/31/2020**
Contract Type: Alliant GWAC Performance Based Service Severable FFP (Labor) LH (Travel-related labor over std work week)	Vendor: CACI NSS, Inc 11955 FREEDOM DR STE 12000 RESTON, VA 20190-5687 United States (703) 434-4137

MODIFICATION SUMMARY

All changes are highlighted in yellow and/or in **bold print**

Mod 01 : **The purpose of this modification is to incorporate incremental funding in the amount of $17,921,306.99 to the Base Period. The Base Period is hereby fully funded in the amount of $23,895,075.99.**

Mod 02: **The purpose of this modification is to Exercise Option Period 1 IAW FAR 52.217-9 Option to Extend the Term of the Contract, and to provide incremental funding in the amount of $3,686,000.**

Mod 03: **The purpose of this modification is to provide the final increment of funding for Option Year 1, IAW FAR 52.212-4 (C) Changes in the amount of 18,916,263.88.**

Mod 04: **The purpose of this modification is to change the company name from L-3 National Security Solutions, Inc to CACI NSS, Inc, pursuant to FAR 42.2 and GSA Modification PA11, Contract: GS00Q09BGD0037 dated 09/20/2016. The Change-of-Name Agreement has been fully executed and is dated 1 February 2016. The address, DUNS, and Cage Code remain the same. This mod also changes the Senior Contracting Officer from Fred Tingle to Delicia McSweeney.**

Mod 05: The purpose of this modification is to bring the manning levels for OY2, OY3, and OY4 to the same level of effort as the Base Period and OY1.

Mod 06: Mod 06: The purpose of this modification is to Exercise Option Period 2 IAW FAR 52.217-9 Option to Extend the Term of the Contract, and to provide funding in the amount of $22,605,583.88.

Mod 07: The purpose of this modification is to:
1. Bring the manning levels for remainder of OY2, OY3, and OY4 to a level that will support US Cyber Command's transition from the Defense Information Assurance Certification and Assurance Program (DIACAP) to the Risk Management Framework (RMF) as identified below.

a. Increase personnel for 5.3.7 (b) (4) positions.
b. Increase personnel for 5.3.17 (b) (4) position.
c. Increase personnel for 5.3.21 (b) (4) positions.
d. Add paragraphs 5.3.24, 5.3.25, and 5.3.26 and provide (b) position for each.
e. Increase personnel for 5.2.10 (b) (4) position.
f. Add paragraphs 5.2.17 and 5.2.18 and provide (b) position for each.
g. Update Appendix F, estimated Government Workload

2. Provide funding for the increase level of support.

Mod 08: The purpose of this modification is to Exercise Option Period 3 IAW FAR 52.217-9 Option to Extend the Term of the Contract, and to provide funding in the amount of $24,219,479.34. This mod also changes the Senior Contracting Officer from Delicia McSweeney to Ronald P Alexander.

Mod 09: The purpose of this modification is to de-obligate funds from OY3 per client request in the amount of: $6,521,173.79.

Mod 010: The purpose of this modification is to provide the final increment of funding for Option Year 3, IAW FAR 52.212-4 (C) Changes.

Mod 011: The purpose of this modification is to:
1.) De-obligate unused funds from the Base Year, Option Year 1, and Option year 2 per the clients request in the amount of: $11,561,887.27.
2.) Change the Senior Contracting Officer from Ronald P Alexander to Rodney C Lewis.
3.) The award value of this task remains unchanged.
4.) All other terms and conditions remain unchanged.

Mod 012: The purpose of this modification is to Exercise Option Year 4 IAW FAR 52.217-9 Option to Extend the Term of the Contract and to provide full funding for OY 4.

TABLE OF CONTENTS

Performance Work Statement

1.0 Introduction and Background

This task order is to provide networking support, help desk support, web master duties, training, technical, project management, administrative, information assurance, cyber, and documentation duties to multiple deployed Southwest Asia Area (SWA) of Responsibility sites for Non-Classified Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network Programs (SIPRNET), ISAF and GCTF. Services provided will improve effectiveness in the planning, training, exercising, executing and assessment of United States Central Command Air Force (USAFCENT)'s mission responsibilities and maintenance of supporting infrastructures within a constantly changing political and military environment. The scope of this task order includes support to the programs, projects and processes employed by USAFCENT to meet existing and future contingency requirements. This task order includes support to Headquarters USAFCENT, deployment locations and subordinate units.

1.1 Organization.

USAFCENT/A6
Network Operations and Security Center (NOSC)
486 Dryden Way, Shaw AFB, SC 29152

1.2 Scope.

The Contractor shall provide USAFCENT/A6 networking support, help desk support, web master duties, training, technical, project management, administrative, information assurance, cyber, and documentation duties to multiple deployed Southwest Asia Area of Responsibility sites for Non-Classified Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network Programs (SIPRNET), ISAF, GCTF, Theater Battle Management System (TBMCS), Coalition Networks, and other Air Force proprietary systems.

2.0 General Information

2.1 Contract Type.

This Task Order is a Performance Based requirement. Requirements contained in the PWS are a Firm Fixed Price (FFP) Hybrid with Labor Hours (LH) and (CR) for Travel, and ODC's.

2.2 Period of Performance.

Duration of this task is one (1) year Base Period and four (4) one (1) year option periods options. There will be a 30 day transition period included within the base period identified below.

Base Year - 4/1/2015 thru 3/31/2016
Option Year 1 - 4/1/2016 thru 3/31/2017
Option Year 2 - 4/1/2017 thru 3/31/2018
Option Year 3 – 4/1/2018 thru 3/31/2019
Option Year 4 – 4/1/2019 thru 3/31/2020

2.3 Place of Performance

Primary work is to be performed on-site, USAFCENT/A6, Bldg 1102, 523 Nelson Ave., or other facilities occupied or used by the Network Operations and Security Center, Shaw Air Force Base, SC. The contractor must be able to work at the NOSC alternate location in Montgomery, Alabama if/when directed by the CRO or representatives for contingency/continuity of operations. These positions are identified in PWS reference 5.2.1 – 5.2.16 and 5.3.1 – 5.3.23.

Primary work is to be performed on site 33NWS/DO; Building 16000 & 2012 at Lackland AFB, Texas. The contractor must be able to work at the 33NWS' alternate operating location (AOL) at Randolph AFB, Texas if/when directed by the 33NWS/DO or his representative for contingency/continuity of operations. These positions are identified in non-deployable positions PWS reference 5.4.1 and 5.4.2

2.4 Hours of Work.

This NOSC is a 24 hour-a-day, 7 day-a-week work center in support of contingency operations in SWA. There are three 8 hour shifts during normal peacetime operation: 0730-1630, 1530-0030, and 2330-0830 (Note: shift times may fluctuate to meet mission requirements). During enhanced contingencies and/or accelerated operations the shift length will increase to 12 hours-a-day for two shifts (times may vary to match the needs of the USAFCENT mission). Contractor employees shall be required to work holidays and weekends, as needed. TDY positions work hours will be adjusted to meet deployed location mission needs; workdays will be for up to 12 work-hours. Travel in the AOR will be considered a normal workday and the Contractor shall charge hours in accordance with the Joint Traffic Regulation.

2.5 Over and Above Standard Work Hours While on Travel/TDY Status.

When contractor employees are on travel/temporary duty (TDY) status in performance of this task order, mission needs may require additional hours beyond the standard 40-hour work-week period. A Labor-Hour line item is included in the task order schedule for hours worked while on travel/temporary duty (TDY) status in excess of 80 hours during any two-week period for each individual contractor employee. The Contractor shall include a list of all employees working any hours in excess of the standard 80 hour work period in each monthly report. The list shall identify each employee and all hours worked in excess of 80 hours over each two-week period, and shall be submitted with each monthly invoice. In this instance, an 80 hour work period is considered 80 hours over a two week period. The contractor shall not exceed the labor hours ceiling identified in the schedule without prior approval from the GSA Contracting Officer. If an increase in the Labor-Hour ceiling identified in the schedule is required, the contractor must

submit a request to the Contracting Officer in accordance with FAR clause 52.232-7.

2.6 Non-Deployment Off-Site Specific Requirements.

All personnel assigned under PWS 5.4.1 and 5.4.2 assigned to NOSC_IA, 33rd Network Warefare Sqn, Lackland AFB TX shall have a TS/SCI clearance.

3 Government/Contractor Furnished Items and Services.

3.1 Government Furnished Items and Services.

3.1.1 The contractor shall utilize standard and specialized equipment, See Appendix C and D. Government Furnished Equipment (GFE) to test and identify problems in order to isolate fault locations and implement corrective actions to restore the LAN operations. NOTE: The fault isolation capability will be to the Lowest Repairable Unit (LRU). Report these deficiencies to the Program Manager and designated Government official, who will recommend administrative actions required to restore maximum system support and availability.

3.1.1.1 Government Provided Equipment for Training Lab Equipment at the NOSC is located in Appendix C.

3.1.1.2 Government Provide Equipment for Contractor Onsite Lab is located in Appendix D. The Contractor shall establish a Secret Internet Protocol Router Network (SIPRNet) collateral integrated test environment located at the Contractor's facility. The Contractor shall install GFE into a dedicated 42 RU rack with a Power Distribution Unit (PDU) in order to establish a secure Integrated Test Environment Lab at the Contractor's site.

3.1.2 Government Provide Phone Access.

The government will provide PIN numbers and associated long distance phone access from the Shaw AFB operating location for the sole purpose of mission completion. This phone access will be utilized to make official long distance telephone calls only.

3.1.3 Government Provided Desktop Computers.

The government will provide contractors with computers and other data devices required to complete all tasks in this tasks order. Contractors will not be allowed to use personal or vendor provided computers on the government network.

3.1.4 Government Provided Laptop Computers.

The government will provide contractors with laptop computers for the sole purpose of TDY operations. This caveat is limited to TDY positions. All other contractors will be provided with desktop computers for use at the Shaw AFB work place.

3.1.5 Government Provided Passports and Immunizations.

Deployable contractor positions require contractors to have a valid passport and current immunizations. The US Government will notify the contractor of visa requirements, the Contractor shall be responsible for obtaining visas for deploying contractor personnel. The Contractor shall be responsible for funding and processing both requirements.

3.1.6 Government Provided US DoD Identification Cards.

All contractors will be provided US DoD Identification Cards, and must be carried at all times while deployed or on a military installation. DoD Identification Cards does not negate the need or requirement for other security badges as required for specific installations and/or deployment to other countries in support of the USAFCENT mission.

3.1.7 Access and Physical Security.

The Government shall assist in arranging access to all Government facilities required for contract performance. Personnel shall comply with NOSC physical security policies and procedures. The NOSC and work centers are controlled environments with restricted access.

3.1.8 Government- Furnished Vehicles.

Transportation requirements will be worked differently at each AOR location and will be determined at each site. The contractor may be required to provide rental vehicles on a reimbursable basis. These rental vehicles will be considered as Government vehicle for the purpose of use. If government vehicles are provided to contract employees, these vehicles are to be used for official use only. At no time shall these vehicles be utilized for personal or unofficial purposes unless specifically authorized by the Contracting Officer. Only one (1) vehicle will be authorized and reimbursed per four (4) OCONUS contract employees.

3.2 Contractor Furnished Items and Services.

3.2.1 Cellular Phones.

The Contractor shall provide cell phones for all personnel in deployable status and personnel requiring on-call or standby duties. On Call TDY personnel cellular phones will have international service and be useable in all Southwest Asia countries where cellular service is available. Cell phones will have the capability to connect to the computer and used for data transfer. While deployed cell phones will only be used for official business; charges determined to be for personal use will not be charged back to the government.

3.2.2 Other items

The Contractor shall obtain certification of contractor employees work hours by assigned COR.

The contractor shall be responsible for pre-deployment and post-deployment medical services to include a fitness physical for each candidate. This examination will include medical history, height, weight, blood pressure, 14-point blood chemistry check, HIV antibody, and chest x-ray.
In the event contractor personnel is unable to perform their duties due to illness or other reasons, the contractor is responsible for providing the name (and all other applicable/necessary

information) of a suitable replacement within 72 hours to USAFCENT/A6, QA and Contracting Officer. The contractor will maintain the capability to place any OCONSUS/TDY personnel in-country within 72 hours, or as soon as USAFCENT/A6 is able to obtain country clearances and fulfill other regulatory and host nation requirements. The contractor shall furnish all necessary immunizations for personnel, not earlier than 30 days prior to their scheduled departure for the reimbursement for services will be required. Immunizations required will be the same, as those required for active duty personnel.

4 Performance Requirements Summary

Table 1.

PWS	Deliverable/Required Service	Performance Standard	Acceptable Quality Level	Method of Surveillance
5.1.1	General Networking Tasks	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.2	LAN Support Tasks	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.3	WAN/Enterprise Support Task	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.4	OS Support Tasks	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.5	Web Based Applications and Servers Task	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.6	Network Security Tasks	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection

5.1.7	Installation Task	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.8	**Documentation Tasks**			
5.1.8.1	Trouble Ticketing System	Delivery within 30 minutes after incident/event	90% On time delivery	Periodic Inspection
5.1.8.2	Trip Reports	Delivery within 5 workdays after meeting	80% On time delivery	Periodic Inspection
5.1.8.3	Project Reports	Delivery within Non-Critical: Weekly Critical: 24 hours	80% On time delivery	100% Inspection
5.1.9	Technical Coordinator Tasks	Completed/Operationalized to meet specific Project Mgt goal timelines	On time delivery Non-Critical: 90%	100% Inspection
5.1.10	Technical Certification Requirements	All Certifications required	100% Certification e	100% Inspection

5 Functional Specific Performance Requirements.

5.1 Core Technical Expertise Tasks and Services.

5.1.1 **General Networking Tasks.**

In support of network operations, contractor personnel must be skilled in network engineering concepts and all layers of the OSI and DOD TCP/IP model. Provide support in the application of network security devices at Tier 0, Tier 1, and Tier 2 of network architecture. Install and maintain the application of network devices such as routers, switches, bridges, and hubs. Contractor shall have a strong understanding of wide area and local area network architectures. Contractor shall apply principles associated with the use of LAN topologies; Bus, Star, Token Ring, etc.

5.1.2 **LAN Support Tasks.**

Contractor shall perform installation and administration of PC and Server in a client-server environment. Optimize LAN operations at both network and systems level. Configure Dynamic Host Control Protocol (DHCP), Windows Internet Naming Service (WINS), Dynamic and Integrated Domain Name Service (DNS), and Active Directory (AD) principles. Apply proper

security measures to safeguard government LAN as closed networks or when integrated in to an Enterprise environment. Contractor shall use Public Key Infrastructure (PKI) technology for network and systems access. Contractor's knowledge of PK Enabled systems will be sufficient to be able to assist deployed users with the migration and daily use of the technology.

5.1.3 **WAN/Enterprise Support Task.**

Contractor shall research, document, and track to resolution all outages, trouble calls, virus outbreaks, and network intrusions. Contractor shall utilize the NOSC toolset to accurately analyze and report on the overall health of local and deployed networks. Contractor shall recommend appropriate changes/resolutions in response to observed trends in Enterprise Level Cisco and Microsoft fault isolation and correction. Contractor shall provide On-the-job training to deploying personnel on network enterprise topology and connectivity. The contractor shall document, and track to resolution all outages, trouble calls, virus outbreaks, and network intrusions. Train local help desk personnel and subordinate contractors on Cisco, Microsoft, and general network troubleshooting. Contractor shall configure and maintain DNS and BIND domain name services on both UNIX and Microsoft platforms. Contractors will understand the function of Certificate Authority (CA), Online Certificate Status Protocol (OCSP), and LEAP server PKI technologies used to support the enterprise.

5.1.4 **OS Support Tasks**

Contractor shall:

5.1.4.1 Microsoft OS. Install, maintain, configure and optimize Microsoft PC and Network Operating Systems, to include XP, Vista, 2000, 2003, 2008, 2012 and future series kernels. Integrate and apply third-party software/applications with Microsoft's OS. Understand AD principles at forest and domain levels, and apply these principles at various levels for of the AD tree, including containers, and leaf objects. Apply and troubleshoot Group Policies Objects (GPO) in an AD environment. Apply applicable security measures to properly safeguard government systems operating Microsoft OS.

5.1.4.2 UNIX OS. Install, configure and optimize multiple Unix Operating Systems including Linux, BSD, Solaris (Sun), and Red Hat (RHEL) for server and PC enterprise operations. Knowledge includes installation, configuration and Optimization. Apply applicable security measures to properly safeguard government systems operating Unix OS.

5.1.4.3 Cisco IOS. Install and configure Cisco routers and switches to provide IP routing and policy routing. Configure routers to accommodate IP tunnels in an enterprise level. Apply applicable security measures to properly safeguard government switches and routers operating Cisco OS.

5.1.4.4 Special and Proprietary OS. Install, configure, and maintain specialty operating systems such as Blue coat proxy, VPN, and TACLANE (SG/KG-175) and KG 250 Encryption devices. Includes OS updates and security patches to optimize performance and ensure security.

5.1.5 **Web Based Applications and Servers Task**.

Provide Webmaster support duties including assistance and support with remote user trouble calls, fault isolation, SSL certificates, and server health to include daily log file reviews. Maintain and troubleshoot basic web pages in HTML and XML format. Create, update, maintain, and remove Microsoft SharePoint Services using webparts and other common SharePoint tools.

5.1.6 **Network Security Tasks**.

Contractor shall administer network and systems using security in-depth models, including detection, and boundary protection. Provide remote network administration and firewall support. Manage and maintain control of network intrusion detection systems. Contractor must utilize firewall and intrusion detection technologies such as sniffing/monitoring, access control list, proxies, IP filters, and syslog review. Contractor must understand and apply knowledge of firewall services, such as DNS and BIND, SMTP, and server redirection to support external and internal networks. Contractor shall understand and apply applicable security measures to properly safeguard government systems, PC, servers, switches, routers, and other devices. Contractor shall ensure the Symantec Antivirus Server (SAV) is properly configured and operational on the SAV and Gateway servers. Contractor shall coordinate with other Systems Engineers to rectify SAV problems. Contractors must be knowledgeable on current Host Based Security Systems such as McAfee Enterprise Policy Orchestrator (ePO) and associated antivirus.

5.1.7 **Installation Task.**

Deployable contractor personnel must possess a valid US Passport, country clearance, visa, be current on all required immunizations, and be certified as deployable by their medical physician. Additional training may be required for individuals to be qualified for volunteer deployment team members. If additional training is required, it will be accomplished in-house or as an existing part of the project.

5.1.8 **Documentation Tasks**.

5.1.8.1 Trouble Ticketing System (TTS). Contractor shall ensure they capture all facts pertaining to trouble calls, fix actions, and assigned tasks, being tracked in the TTS. All

comments will remain professional at all times. Other associated and relative documents shall also be attached to the trouble ticket.

5.1.8.2 Trip Reporting. Contractor personnel shall provide a fully documented trip reports within five duty days of return. Trip reports will be provided for all Conferences, Seminars, In-Progress Reviews, Technical Develop and Engineering Studies. Trip reports will be in standard AF format and delivered to the Chief of supported section for review. A copy of the report shall also be uploaded to ITSS.

5.1.8.3 Project Reporting. Contractor shall ensure that all project updates will be completed and submitted using Microsoft Project Server as the basic systems of record for Project management. Project inputs will be collected continuously and entered into the system on a daily basis time permitting; however, projects will be updated no later than by close of business on Friday of each week.

5.1.9 **Technical Coordinator Tasks**.

Contractor must coordinate work and workflow requirements with senior engineer and/or management staff. Contractor employees must work independently, without supervision to successfully resolve problems or meet task objects.

5.1.10 **Technical Certification Requirements**.

Contractor personnel must hold, maintain, and upgrade certification in the following areas and/or show equivalent expertise. In exceptional and rare circumstances the contractor employer may submit contractor personnel for consideration grant a temporary waiver of certification if the contractor can demonstrate to the Client Representative's satisfaction that the employee in question has sufficient mastery of the matter which is the subject of the certification; however, the duration of the waiver will be only as long as is necessary for the employee to obtain the certification and in no circumstances shall exceed six months. The following is a table of the Required Technical Certifications:

Table 2

Index	Certificate Description	Position
1	Microsoft Certified Professional (MCP) Desktop	5.2.16
2	Microsoft Certified Professional MCP Server	5.2.6, 5.2.7
3	Microsoft Certified Professional MCP Lync	5.3.7
4	Microsoft Certified Professional (MCP) SCCM	5.2.8, 5.2.9, 5.3.26
5	Microsoft Certified Professional (MCP) Project Server	5.2.2, 5.2.17
6	Microsoft Certified Solutions Associate (MCSA)	5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.3.12, 5.3.13, 5.3.15
7	Microsoft Certified Solutions Expert (MCSE) Server Infastructure1	5.2.5, 5.2.14, 5.3.1, 5.3.5, 5.3.11, 5.3.14,

		5.3.16, 5.3.21, 5.3.26
8	Microsoft Certified Solutions Expert(MCSE) Exchange1	5.3.7
9	Microsoft Certified Solutions Developer (MCSD) Application Builder1	5.3.17, 5.3.18, 5.3.23
10	Microsoft Certified Solutions Expert (MCSE) Data Management and Analytics1	
11	Microsoft Certified Trainer	5.3.5, 5.3.26
12	Cisco SourceFire Certification	5.3.12
13	Cisco Certified Network Associate (CCNA) Routing and Switching	5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.10, 5.2.11, 5.3.11, 5.3.15, 5.3.16
14	Cisco Certified Network Associate (CCNA) Security	5.2.13, 5.3.1
15	Cisco Certified Network Professional (CCNP) Routing and Switching3	5.2.14, 5.3.5, 5.3.13, 5.3.14, 5.3.24, 5.3.26
16	Cisco Certified Network Professional (CCNP) Security3	5.3.12
17	Cisco Certified Network Professional3 (CCNP) Collaboration	5.3.25
18	Cisco Certified Internetworking Expert[2] (CCIE)2	5.3.13, 5.3.24, 5.3.25
19	Firewall Certified/Trained Engineer[9]	5.2.5, 5.2.6, 5.2.7,5.2.10, 5.2.11, 5.2.13, 5.2.14, 5.2.15, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.11, 5.3.12, 5.3.15, 5.3.14, 5.3.16, 5.3.24, 5.3.25, 5.3.26
20	FortiGate Network Security Professional (NSE)	5.2.14, 5.3.5, 5.3.13, 5.3.14, 5.3.26
21	Assured Compliance Assessment Solution (ACAS)	5.3.1
22	Host Based Security System (HBSS)	5.2.5, 5.2.14, 5.3.14, 5.3.21
23	CompTIA Security+	5.2.2, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.10, 5.2.11, 5.2.13, 5.2.14, 5.2.15, 5.2.16, 5.2.17, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7, 5.3.8, 5.3.9, 5.3.10, 5.3.15, 5.3.16, 5.3.17, 5.3.18, 5.3.19, 5.3.20,5.3.21, 5.3.22, 5.3.24, 5.3.25, 5.4.1
24	CompTIA Network+	5.2.15, 5.4.1
25	CompTIA A+	5.2.8, 5.2.9, 5.2.16,
26	VMware Certified Associate (VCA)	5.2.5, 5.2.14, 5.3.5,

		5.3.12, 5.3.13, 5.3.14, 5.3.21
27	EC-Council Certified Ethical Hacking (CEH)	5.2.13, 5.3.15, 5.3.16, 5.4.1, 5.4.2
28	Technical Instructional Certification[4]	5.3.5, 5.3.26
29	Unix Certification[5]	5.2.4, 5.2.5, 5.2.7, 5.2.9, 5.2.10, 5.2.13, 5.2.14, 5.3.5, 5.3.12
30	Certified Information Systems Security Professional (CISSP)	5.2.18, 5.3.1, 5.3.11, 5.3.12, 5.3.13, 5.3.14, 5.3.23, 5.3.26, 5.4.2
31	SolarWinds Certified Professional (SCP)	5.2.9, 5.2.10
32	Certified Associate in Project Management (CAPM)	5.2.17
33	Project Management Professional (PMP)	5.2.2
34	Information Technology Infrastructure Library (ITIL)	All
35	Bachelor's Degree (BA or BS) in Information Systems, Information Technologies, or Computer Science[6]	5.2.2, 5.2.9, 5.2.11, 5.2.13, 5.2.14, 5.2.18, 5.3.1, 5.3.5, 5.3.11, 5.3.12, 5.3.13, 5.3.16, 5.3.18, 5.4.2
36	Master's Degree in Information Systems, Information Technologies, or Computer Science[7]	5.3.14, 5.3.23, 5.3.26
37	Forklift Drivers Licenses[8]	5.2.3, 5.2.12,
38	DoD 8570 Requirement 11	All Personnel With Elevated Admin Rights

[1] May be waived with equivalent Microsoft experience and expertise prior to employment, candidate must obtain MCSE within 6 months of employment, and maintain a current MCSE that is no less than one iteration back from current NOSC deployed servers .
[2] Due to limited availability, the Client may choose to waiver CCIE certification for individuals with Cisco Certified Network Professional (CCNP) and sufficient/equivalent experience
[3] A CCIE certification will override any Cisco Certified Network Professional (CCNP) requirement.
[4] CITT, MCT, or Military Equivalent
[5] The client can wavier this certification if equivalent 5 years of UNIX experience.
[6] May be temporarily waived, however candidate must be capable of obtaining Bachelor's Degree within 24 months
[7] May be temporarily waived, however candidate must have Bachelor's Degree (BA or BS) in similar discipline working on Post Graduate degree in an IT area of study, not more than 18 months
[8] Government Drivers Licenses for forklift (up to 10 ton All Terrain [AT]), standard two and four-wheel pickup truck, 2.5 and 5 ton trucks, and other as required
[9] Firewall Certification can be waivered with 2 years' experience on current firewall platform or attending NOSC Firewall class

[10] Cisco Certification or minimum 5 years' experience on intrusion detection system that is currently used by DoD agencies.

[11] DoD 8570 Certification required commensurate with normal assigned duties provided individual is required an administration account.

5.2 USAFCENT Non-Deployment Tasks

5.2.1 Information Technology/Knowledge Management Administrative Specialist (Non-Deployable) Secret

- Contractor shall:
- Develop and prepare technical reports, briefs, and other documents in support the NOSC staff.
- Maintain an action-tracking database on all incoming and outgoing correspondence and/or suspense items in support of the NOSC staff. Correspondence may include but not limited to that which is addressed to and from USAFCENT, 9 AF Headquarters, 609th Air Communications Squadron, and other external agencies or activities.
- Maintain libraries for software, technical manuals, and commercial books.
- Manage knowledge and information resources (information and related resources such as personnel, equipment, funds and related technology) to accomplish organization's mission.
- Responsible for the information and knowledge life-cycle management; including the creation, collection, access storage, retrieval, and disposal of all information originated and received by the NOSC.
- Control creation and ensure efficient use of IT Project management toolset for forms, reports, documentation graphs, charts, and PowerPoint.
- Coordinate with USG IT Project manager and IT Project Engineers for using office automation and information systems (Stand alone and networked) to create, collect, use, access, disseminate, maintain and dispose of information, ensure office supplies are available.
- Convert Word and Email based correspondence into Automated Message Handling Systems (AMHS) message format suitable for official release.
- Maintain SharePoint list and document libraries to ensure office records and working papers comply with AFCENT, AF, CENTCOM, and DoD document management and storage directives.
- Coordinate on security access for all NOSC visitors, include coordination on clearance and issuance of appropriate access facility badges; manage personnel database associates with the automated entry control systems.
- Maintain Division Chiefs calendar and manage incoming tasks from higher headquarters

5.2.1.1 **Documentation Task.** Contractor shall prepare IT Concept of Operations, Engineering plans and other IT communications and correspondence. Contractor shall track electronic and paper IT documentation and coordinate through its life-cycle. Review, evaluate, and edit completed work for accuracy, adequacy, and compliance with policies, systems, methods, and standard practices. Proof read and grammar check all documentation for accuracy.

5.2.1.2 **Technical Coordinator Task** (See Section 5.1.9 Core Expertise) Contractor shall work with the USG Senior Management and Project Leads to coordinate NOSC IT Project personnel issues, to include TDYs, Leave, and official functions. Maintain a master Gantt chart of NOSC events to include NOSC resource critical path.

5.2.1.3 **Workgroup Administrator Support Task**. Install and configure computer operating systems (Windows 7 and future versions). Install, configure, and use software applications such as Word, Excel, Power Point, and Access. Perform basic LAN troubleshooting to determine and verify network capabilities of PCs.

5.2.1.4 **Library Management Task**: Establish, monitor, and maintain management oversight of software and technical manual libraries.

5.2.1.5 **Security Control Task**: Ensures the Automated Entry Control System database and Access Control Lists are current and old/obsolete accounts are removed in a timely manner.

5.2.1.6 **Maintains NOSC Calendar and Task List Task**: Accesses the Division Chiefs calendar and maintains higher headquarters tasking to ensure major events and visits, and tasks are appropriately coordinated to prevent conflict and missed suspenses.

5.2.1.7 **Records Management Task**: Prepare automated file maintenance disposition plans, and electronic records keeping. Perform functional area records manager duties.

5.2.1.8 **Subject Matter Expertise Task**: The Contractor shall provide expertise in the following areas:

a. Air Force publications and forms management pertaining to IT Project to include preparing, controlling, and processing written communications.
b. Office automation equipment
c. Administrative Joint, Air Force, Major Command, Organizational, and Local Operating Instructions

5.2.2 **Senior Information Technology Project Manager (Non-Deployable) Secret**

- Contractor shall:

- Have extensive Project Management background with specific experience with Microsoft Project and Project Server to manage network infrastructure, software development, and other information systems and technology projects.
- Develop project plans, material acquisitions, time management, and detailed project action plans.
- Coordinate each new project with the project leads to customize the project plan to meet specific manning, time, and budget resources.
- Provide project management oversight of information systems and technology projects from inception to completion.
- Maintain a master copy of list of materials for equipment used for each project to preserve standardization of equipment and software across the enterprise. Contractor shall maintain enterprise-level licensing inventory for initial project software, renewals, and upgrades.

- Manage and assist with coordination of IT contracts with GSA and Local Contracting offices for the acquisition of materials, equipment and services.
- Track project resources requests, Request for Quotes (RFQ), Request for Proposal (RFP), and Statements of Work (SOW).
- Install, configure, administer, and maintain Microsoft Project Server and other Web pages to provide access to project status, documentation, and related web-based products.
- Produce detailed professional reports, to brief status of projects to senior leaders, and provide statistical analysis for strategic planning and funding.

5.2.2.1 **Project Plan Development Task**: Contractor shall develop detailed project plans showing assigned resources, materials required, estimated milestone dates, and other relevant details to each specific project. Contractor shall train NOSC personnel on the use and implementation of planning tools and on how to use these planning tools to better implement and track their projects. Contractor shall recommend areas that need improvement and provide metrics to the effectiveness of the plan and resources utilized. Contractor shall capture project data and make it available via the web to all end users and local agencies. Contractor shall be familiarity with information systems and technology.

5.2.2.2 **Project Resource Acquisition Task**: Contractor shall manage the acquisition of associated resources (documentation, licensing, hardware, software, and other materials) required for each task through established funding procedures. Task involves compiling resource requirements from project engineers and assisting with converting those requirements into a purchase order requirements package. Contractor shall adhere to local procedures and regulations when purchasing said resources. Additionally, the project manager will compile project resources, manage storage of project resources, and coordinate shipment of project materials. All purchases will be reviewed, approved, and completed by Government representative prior to obligation and/or fulfillment.

5.2.2.3 **Web Based Applications and Servers Task:** (See Section 5.1.5 Core Expertise) Contractor shall maintain a Project Management web page to access Microsoft Project Server and other Web pages to provide access to project status, documentation, and

related web-based products. Contractor shall coordinate with the web development team for web server support.

5.2.2.4 **Documentation Task**: Contractor shall document entire project in web format (soft copy available to all interested and applicable parties) and in archive format. Contractor shall coordinate the development of a file plan and implement the plan in order to archive all project related data for posterity and future reference. The file plan must conform to Air Force regulations and must include official archival, reviews, inspections, and proper classification markings in accordance with local and Air Force policy.

5.2.2.5 **Technical Coordinator Task:** (See Section 5.1.9 Core Expertise): Contractor shall coordinate with internal and external agencies for the successful execution of project timeline elements. Coordination will include but is not limited to: Concept of Operations (CONOPS), Network Security Certifications, Country Clearance submissions and tracking, personnel movements, and project material acquisitions to include staging and build up of equipment. Coordination will be documented in appropriate project software and maintained for historical and audit purposes.

5.2.2.6 **Technical Certifications Requirements** (See Section 5.1.10 Core Expertise)

5.2.2.7 **Educational Requirements** (See Section 5.1.10 Core Expertise)

5.2.3 **Information Technology Project Management and Logistics (Non-Deployable) Secret**

- Contractor shall:
- Coordinate IT Logistical support of network and systems projects.
- Provide resource planning and materials control as associated with all aspects of this task order.
- Provide logistical support to include shipping, scheduling, planning and implementation, assisting with material procurement and inventory processing, multi-vendor shipping, and coordination of all phases of the IT project.
- Manage just-in-time (JIT) stock levels as they pertain to IT projects, ensures sufficient baseline materials are available for projects.
- Use Microsoft Project and related web-based products to track resources and overall project status.
- Produce detailed professional reports, to brief status of projects to senior leaders, and to provide statistical analysis for strategic planning and funding.
- Function as the alternate IT Project Manager, to maintain the Microsoft Project Server and web pages.

5.2.3.1 **Shipping Plan Development Task**: Contractor shall develop detailed project shipping plans to use the best method for shipping IT equipment and project materials to all countries in the USAFCENT Area of responsibility (AOR). Contractor shall coordinate with the Project Manger and Project Team leads to schedule training of NOSC personnel on the shipping methods and procedures to increase project efficiency. Contractor shall move and/or coordinate the movement of project equipment and materials to the transportation delivery points, both commercial and DoD as required to guarantee delivery. Contractor is responsible for the completion and filing of form DD 1149 and the input of shipping information and data into standard (Remedy) trouble ticketing system (TTS). Contractor shall be familiar with applicable/associated processes and technology. Contractor shall recommend areas that need improvement and provide metrics to the effectiveness of the plan and resources utilized. Contractor shall capture this data and make it available via the web to all end users and local agencies.

5.2.3.2 **Material Processing and Inventory Management and Coordination Task**: Contractor shall manage IT project warehouse and project equipment and materials. This management will include receiving, processing, labeling, correlating, and safeguarding all project equipment and materials. Contractor shall function as the lead shipping coordinator for the movement of project equipment and materials to the transportation delivery points, both commercial and DoD. Contractor shall maintain a database of project materials using automated inventory management database and scanning systems.

5.2.3.3 **Project Stakeholders Timelines Task:** Contractor shall coordinate with internal and external agencies for the successful execution of project timeline elements. Coordination includes, but is not limited to: Providing project manager and project leaders with inputs on inventory and shipping issues for inclusion in the Concept of Operations (CONOPS). Maintaining current country clearance and customs requirements for shipping project materials to insure adequate time is allocated for staging and build up of equipment. Coordination must be documented and maintained by the contractor in appropriate project software for historical and audit purposes.

5.2.3.4 **Multi-vendor Shipping Resource Coordination Task**: Contractor must ensure shipping resources and funds are available for the shipping of IT project equipment and materials. Contractor shall track the expenditure of shipping funds and provide reports to the Project Manager on the funds balance. All purchases will be reviewed,approved, and completed by Government representative prior to obligation and/or fulfillment.

5.2.3.5 **Project Documentation Task**: Contractor shall document all storage warehousing, shipping and reporting associated with the IT project in web format (soft copy available to all interested and applicable parties) and in archive format. Contractor shall coordinate the development of a file plan and implement the plan in order to archive all project related data for posterity and future reference. This file plan must conform to Air Force regulations and must include official archival, reviews, inspections, and proper classification markings in accordance with local and Air force policy.

5.2.3.6 **Documentation Task**: (See Section 5.1.8 Core Expertise): Contractor shall be the alternate IT Equipment Custodian and ensure project materials are properly accounted for on a master inventory database. Contractor shall coordinate the completion of transportation tracking documents, and maintain file copies of transportation control documents in accordance with file plan disposition. Contractor shall send shipping notices to destination POC and open/update a Remedy Trouble Ticket for tracking purposes.

5.2.3.7 **Technical Coordinator Task**: (See Section 5.1.9 Core Expertise): Contractor shall coordinate with internal and external agencies for the tracking and delivery of IT project materials. Contractor shall coordinate domestic and international shipping, to include host nation customs documents and clearance requirements.

5.2.3.8 **Technical Certifications Requirements**: (See Section 5.1.10 Core Expertise)

5.2.4 **Information Technology Technical Writing/Documentation (Non-Deployable) Secret**

- Contractor shall:
- Develop technical documents based on extensive networking background in system administration or network engineering.
- Use provided source document to write systems security accreditation and certification requirement packages in accordance with applicable Air Force regulations and procedures; including documenting systems architecture and networks' physical layout in writing and graphical presentations.
- Analyze, evaluate, and determine the application of Air Force systems accreditation and certification procedures in relation to existing and planned 9AF/USAFCENT network architecture at Shaw AFB and SWA.
- Predict possible impact of installing new software and hardware in an existing network enterprise.
- Research network topology via NOSC automated toolset (Openview, eHealth, etc) to ascertain connectivity, topology, and status to document processes and logic diagrams for regularly accomplished tasks on the NOSC operations floor as well as processes utilized by support technicians, typically referred to as Knowledge Books.
- Develop and manage all phases of the documentation project(s) including initial analysis, information gathering, design of deliverables, and distribution of finished product.
- Assist other government and contract personnel with project documentation and web site development as needed
- Assist the Training Manager with standardization and transcription of training materials.
- Assist with tracking and maintain a record of all software licenses for USAFCENT Enterprise software.

5.2.4.1 **General Networking Task**: (See Section 5.1.1 Core Expertise): Contractor shall maintain a standard set of published network architectural diagrams; establish and coordinate periodic reviews and publishing to keep information accurate for use by Network Engineers and Helpdesk Technicians. Contractor shall ensure Enterprise and Site network architecture

drawings and diagrams are up to date and accurate. Establish and maintain a web page to provide deployed sites up/download access for site-specific drawings and diagrams.

5.2.4.2 **LAN Support Task**: Contractor shall understand the use of Dynamic Host Control Protocol (DHCP), Windows Internet Naming Service (WINS), Dynamic and Integrated Domain Name Service (DNS), and Active Directory (AD) principles and integrate these technologies into standard technical references.

5.2.4.3 **WAN/Enterprise Support Task**: Contractor shall develop logic flow charts for Enterprise processes utilized by the NOSC and deployed sites. Provide standardized written procedures and/or checklists for associated with common tasks and procedures.

5.2.4.4 **OS Support Task**: Contractor must understand the basics of the Microsoft, UNIX, and Cisco OS.

5.2.4.5 **Web Based Applications and Servers Task**: (See Section 5.1.5 Core Expertise)

5.2.4.6 **Network Security Task**: (See Section 5.1.6.3 Core Expertise)

5.2.4.7 **Documentation Task**: (See Section 5.1.8 Core Expertise): Contractor shall transfer rough draft technical documentation into a standard document format for formal publishing. Contractor shall work with Network Engineers and Project Leads to document Concept of Operations, Engineering Plans, and Tactics, Techniques and Procedures (TTPs). Contractor shall establish and coordinate an annual review of published documentation. Develop logic flow charts for processes utilized by the NOSC and deployed sites. Provide standardized written procedures and/or checklists for associated with common tasks and procedures. Function as lead reviewer and coordinates a semi-annual review of the Special Instructions for Communicators (SINC).

5.2.4.8 **Technical Coordinator Task**: (See Section 5.1.9 Core Expertise): Contractor shall aid the Training Manager by standardizing training material. Review Remedy trouble tickets and create a knowledge base utilized by the level help desk technicians for fault isolation and resolution

5.2.4.9 **Technical Certifications Requirements**: (See Section 5.1.10 Core Expertise)

5.2.5 **Senior Systems/Network Engineer Subject Matter Expert (SME) (Non-Deployable) Secret**

- Contractor shall:
- Troubleshoot and develop solutions for network anomalies both remotely and locally.
- Analyze a myriad of networking metrics and recognize sub-standard network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.

- Operate network protection and intrusion devices specific to the Department of Defense as well as many commercial information assurance tools.
- Demonstrate strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco, Microsoft, and hardware troubleshooting disciplines.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Direct, organize, and utilize crisis management processes and techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of technical skill sets tempered with confidence, leadership, and management capabilities to support the NOSC Operations Crew Commander.

5.2.5.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.5.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.5.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.5.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.5.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.5.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.5.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor shall provide direct or over-the-shoulder assistance as required using a variety of technologies as appropriate to the task.

5.2.5.8 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents to explain abstract technologies and special interest items in easy to understand termination and examples. The Contractor shall also develop complex and complete tactics, techniques, and procedures (TTPs) on technologies and applications.

5.2.5.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall provide technical support to other Subject Matter Experts/Engineers on a wide variety of technologies and applications.

5.2.5.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.2.6 **Network Engineering Support (Non-Deployable) Secret**

- Contractor shall:
- Use a broad LAN/WAN background to troubleshoot and develop solutions for network anomalies.

- Collect networking metrics for analysis to determine sub-standard network performance.
- Use extensive network troubleshooting experience focused on enterprise-level server farms and advanced server concepts such as firewalls, proxies, and caching arrays.
- Report system and network documented finds to Senior SME for analysis and trending of bandwidth and network security incidents.
- Operate network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools.
- Provide first-level technical support to deployed users, escalates complex problems to Senior SMEs.

5.2.6.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.6.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.6.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.6.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.6.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.6.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.6.7 Documentation Task (See Section 5.1.8 Core Expertise)

5.2.6.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.2.6.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.7 **Firewall Engineering Support (Non-Deployable) Secret**

- Contractor shall:
- Troubleshoot and develop solutions for network anomalies. The Contractor shall analyze a myriad of networking metrics and recognize sub-standard network performance.
- Provide individual(s) who have extensive network troubleshooting experience focused on enterprise-level server farms and advanced server concepts such as firewalls, proxies, and caching arrays.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Operate network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools.
- Document trouble calls utilizing remedy and other tools provided.
- Escalate calls to appropriate help desk level locally or remotely at Secure computing for resolution.
- Research, document, and track to resolution all outages, trouble calls, and network intrusions.

- Utilize the Firewall toolset to accurately analyze and report on the overall health of local and deployed firewalls.
- Enterprise Level firewall fault isolation and correction to include troubleshooting ACLs affecting other network traffic.
- Perform local installation and local and remote administration of firewalls to include command line and GUI interfaces.

5.2.7.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.7.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.7.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)
Contractor shall provide guidance and remote administration in the following areas related to Sidewinder and the Command Center (CC):

a. General Optimization
b. VPN connections between firewalls (Point to Point)
c. ACL management
d. IP Filter management
e. Log analysis
f. Installation
g. Cloning
h. One-to-many – Failover

5.2.7.4 OS Support Tasks (See Section 5.1.4 Core Expertise): Open BSD OS - Contractor shall troubleshoot firewall issues including permissions and type enforcement. Assist remote users through successful backups and restoration actions, and accomplish the same locally.

5.2.7.5 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.7.6 Documentation Task (See Section 5.1.8 Core Expertise)

5.2.7.7 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.2.7.8 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.8 **Network/Systems Configuration Management (Non-Deployable) Secret**

- Contractor shall:

- Use extensive LAN/WAN background and experience to understand systems and network architecture configurations.
- Establish and support the AFCENT Configuration Control Board (CCB) in accordance with Joint, CENTCOM, AF, and local Operating Instructions.
- Provide functional management of the CCB, coordinate place and time of the CCB with the board president and other voting members, collect and publish agenda items, record meeting minutes, and publish information on a secure web page.
- Monitor, processes, and manage the Systems Requirements Documents (AF3215) utilizing BMC Remedy (PWRR+) and other USAF and/or DoD software supporting the AFCENT mission.
- Review and coordinate all NOSC Communications Task Orders (CTO) submissions, and release to AFCENT Fwd for publishing.
- Check all systems and network standard processes through performance evaluation for technical accuracy and viability.

- Ensure Special Instructions for Communicators (SPIN-C) submissions are technically accurate and up-to-date.

- General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.8.1 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.8.2 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.8.3 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.8.4 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.8.5 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.8.6 Documentation Task (See Section 5.1.8 Core Expertise)

5.2.8.7 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.2.8.8 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.9 **Senior Network/Systems Configuration Management (Non-Deployable) – Top Secret**

- Contractor shall:
- Use extensive LAN/WAN background and experience to understand systems and network architecture configurations.
- Establish and support the AFCENT Configuration Control Board (CCB) in accordance with Joint, CENTCOM, AF, and local Operating Instructions.

- Provide functional management of the CCB, coordinate place and time of the CCB with the board president and other voting members, collect and publish agenda items, record meeting minutes, and publish information on a secure web page.
- Monitor, processes, and manage the Systems Requirements Documents (AF3215) utilizing BMC Remedy (PWRR+) and other USAF and/or DoD software supporting the AFCENT mission.
- Review and coordinate all NOSC Communications Task Orders (CTO) submissions, and release to AFCENT Fwd for publishing.
- Check all systems and network standard processes through performance evaluation for technical accuracy and viability.
- Ensure Special Instructions for Communicators (SPIN-C) submissions are technically accurate and up-to-date.

5.2.9.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.9.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.9.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.9.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.9.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.9.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.9.7 Documentation Task (See Section 5.1.8 Core Expertise)

5.2.9.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.2.9.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.9.10 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.2.10 **Network/Systems Performance and Analysis (Non-Deployable) Secret**

- Contractor shall:
- Analyze a wide array of networking metrics collected from the NOSC standard network management toolset to determine the state of the network.
- Provide recommendations on performance of network management toolset, and use Remedy Trouble Ticketing System to report any problems to systems administrators.
- Develop reports and trend analysis documentation supported with graphs and charts to illustrate bandwidth throughput and utilization based on specific ports and protocols.

- Utilize data to make expert decisions and recommendations on how to optimize network performance.
- Manage the Site/Aggregated Bandwidth Matrix to be provided to senior IT managers for review, provides analysis as required.
- Analyze data routing ensure networks are utilizing located bandwidth, make recommendations to alter transmission systems to enhance network performance or to provide redundancy, reliability, or survivability.

5.2.10.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.10.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.10.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.10.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.10.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.10.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.10.7 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall submit daily performance reports and ensures automates performance tools are functioning correctly. Use databases and spreadsheets to manage data for performance analysis. Manage files storage and safeguard data.

5.2.10.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall coordinate all efforts closely with Modeling and Simulation, Information Assurance, and Networks to prevent overlap or conflicts of efforts, and the delivery on a single performance report daily.

5.2.10.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.11 **Senior Network/Systems Performance (Non-Deployable) TS**

- Contractor shall:
- Analyze a wide array of networking metrics collected from the NOSC standard network management toolset to determine the state of the network.
- Provide recommendations on performance of network management toolset, and use Remedy Trouble Ticketing System to report any problems to systems administrators.
- Develop reports and trend analysis documentation supported with graphs and charts to illustrate bandwidth throughput and utilization based on specific ports and protocols.
- Utilize data to make expert decisions and recommendations on how to optimize network performance.
- Manage the Site/Aggregated Bandwidth Matrix to be provided to senior IT managers for review, provides analysis as required.

- Analyze data routing ensure networks are utilizing located bandwidth, makes recommendations to alter transmission systems to enhance network performance or to provide redundancy, reliability, or survivability.

5.2.11.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.11.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.11.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.11.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.11.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.11.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.11.7 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall submit daily performance reports and ensures automates performance tools are functioning correctly. Use databases and spreadsheets to manage data for performance analysis. Manage files storage and safeguards data.

5.2.11.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall coordinate all efforts closely with Modeling and Simulation, Information Assurance, and Networks to prevent overlap or conflicts of efforts, and the delivery on a single performance report daily.

5.2.11.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.11.10 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.2.12 **Information Technology Logistics Asset Management and Recovery (Non-Deployable) Secret**

- Contractor shall:
- Coordinate IT Logistical support of network and systems projects.
- Provide resource planning and materials control as associated with all aspects of this task order.
- Provide logistical support to include shipping, scheduling, planning and implementation, assisting with material procurement and inventory processing, multi-vendor shipping, and coordination of all phases of the IT project.

- Manage just-in-time (JIT) stock levels as they pertain to IT projects, ensures sufficient baseline materials are available for projects.
- Use IT bar code resource management systems to actively manage the transfer of IT resources between the NOSC and deployed forces.
- Produce detailed professional reports, to brief status of projects to senior leaders, and to provide statistical analysis for strategic planning and funding.
- Track resource availability reports to the IT Project Manager.
- Use the Air Force Integrated Technology Asset Management Systems (ITAMS), or other successor systems to manage IT project resources.
- Be the NOSC IT Equipment Account/Control Manager.

5.2.12.1 **Shipping Plan Development Task:** Contractor shall develop detailed project shipping plans to use the best method for shipping IT equipment and project materials to all countries in the USAFCENT Area of responsibility (AOR). Contractor shall coordinate with the Project Manger and Project Team leads to schedule training of NOSC personnel on the shipping methods and procedures to increase project efficiency. Contractor shall move and/or coordinate the movement of project equipment and materials to the transportation delivery points, both commercial and DoD as required to guarantee delivery. Contractor is responsible for the completion and filing of form DD 1149 and the input of shipping information and data into standard (Remedy) trouble ticketing system (TTS). Contractor shall be familiar with applicable/associated processes and technology. Contractor shall recommend areas that need improvement and provide metrics to the effectiveness of the plan and resources utilized. Contractor shall capture this data and make it available via the web to all end users and local agencies.

5.2.12.2 **Material Processing and Inventory Management and Coordination Task:** Contractor shall manage IT project warehouse and project equipment and materials. This management will include receiving, processing, labeling, correlating, and safeguarding all project equipment and materials. Contractor shall function as the lead shipping coordinator for the movement of project equipment and materials to the transportation delivery points, both commercial and DoD. Contractor shall maintain a database of project materials using automated inventory management database and scanning systems.

5.2.12.3 **Equipment Custodian Task:** Contractor shall be the primary IT Equipment Custodian for all NOSC accounts and use local IT databases and the Integrated Technology Asset Management Systems (ITAMS) database to issue, receive, and recover IT project equipment.

5.2.12.4 **Project Stakeholders Timelines Task:** Contractor shall coordinate with internal and external agencies for the successful execution of project timeline elements. Coordination includes, but is not limited to: Providing project manager and project leaders with inputs on inventory and shipping issues for inclusion in the Concept of Operations (CONOPS). Maintaining current country clearance and customs requirements for shipping project materials to insure adequate time is allocated for staging and build up of equipment. Coordination must be documented and maintained by the contractor in appropriate project software for historical and audit purposes.

5.2.12.5 **Multi-vendor Shipping Resource Coordination Task**: Contractor must ensure shipping resources and funds are available for the shipping of IT project equipment and

materials. Contractor shall track the expenditure of shipping funds and provide reports to the Project Manager on the funds balance. All purchases will be reviewed and approved by Government representative prior to obligation and/or fulfillment.

5.2.12.6 **Project Documentation Task**: Contractor shall document all storage warehousing, shipping and reporting associated with the IT project in web format (soft copy available to all interested and applicable parties) and in archive format. Contractor shall coordinate the development of a file plan and implement the plan in order to archive all project related data for posterity and future reference. This file plan must conform to Air Force regulations and must include official archival, reviews, inspections, and proper classification markings in accordance with local and Air force policy.

5.2.12.7 **Documentation Task**: (See Section 5.1.8 Core Expertise): Contractor shall use bar-coding technologies to ensure project materials are properly accounted for on a master inventory database. Contractor shall coordinate the completion of transportation tracking documents, and maintain file copies of transportation control documents in accordance with file plan disposition. Contractor shall send shipping notices to destination POC and open/update a Remedy Trouble Ticket for tracking purposes.

5.2.12.8 **Technical Coordinator Task**: (See Section 5.1.9 Core Expertise): Contractor shall coordinate with internal and external agencies for the tracking and delivery of IT project materials. Contractor shall coordinate domestic and international shipping, to include host nation customs documents and clearance requirements.

5.2.12.9 **Technical Certifications Requirements**: (See Section 5.1.10 Core Expertise)

5.2.13 **Cyber Intelligence Analyst/Coordinator (Non-Deployable) TS/SCI**

- Contractor shall:
- Analyze cyber intelligence reports to determine correlation and applicability to network operations on AFCENT networks.
- Analyze network intrusion detection reports and vulnerability assessments to evaluate security posture as it pertains to current operations and information security levels.
- Recommends security posture changes based on security analysis and changes in threat indicators.
- Develop reports and trend analysis of internal and external security activity, and incidents.
- Provide on-shift training for both contractors and government personnel to include analysis interpretation and threat/event correlation.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network security problems/issues.

5.2.13.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.13.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.13.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.13.4 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.13.5 Cyber Data Analysis Tasks: Contractor analyze Suspicious Event Reports (SER) to determine the impact and affect on AFCENT's networks and systems, and provide details on possible actions and alternatives to resolve problems, issues, attacks, and intrusions.

5.2.13.6 Cyber Intelligence Coordination Task: Contractor shall coordinate with intelligence activities to gain situational awareness of cyber and security threats. Coordination will include physical and virtual meetings, using voice and video technologies. The contractor shall develop a weekly Cyber Activity Report focused on AFCENT's networks; the report will include intelligence that directly and indirectly affects AFCENT's networks and operations from both red and blue team perspectives.

5.2.13.7 Intrusion Detection Task: Contractor shall examine logs and information gained from network sniffers or protocol analyzers to determine if possible outside or unauthorized access has occurred. Track and record possible intrusion or security breach from routine daily analysis to successful anomaly/intrusion identification, which includes writing detailed analysis for possible legal use. Function as government subject matter security expert for any legal actions associated with security breaches.

5.2.13.8 Vulnerability Assessment Task: Contractor shall use vulnerability assessment reports to analyze networks and operation systems to determine security weaknesses and shortfalls. Research and provide detailed fix actions for all identified vulnerabilities. Coordinate with other computer emergency response teams (CERT) to ensure latest known vulnerabilities are properly identified and corrected. Make recommendations for changes in security policy based on vulnerability assessments.

5.2.13.9 Documentation Task (See Section 5.1.8 Core Expertise)

5.2.13.10 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.2.13.11 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.13.12 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.13.13 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.13.14 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.13.15 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.13.16 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.13.17 Network Security Tasks (See Section 5.1.6 Core Expertise): Contractor shall document, create, maintain, and track network accreditation packages throughout their life cycle for local and deployed networks. Work with the Web Design Engineer and Programmer to provide access to the accreditation documentation using standard NOSC web page design practices.

5.2.13.18 Reserved

5.2.13.19 Reserved

5.2.13.20 Reserved

5.2.13.21Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.2.13.22 Educational Requirements (See Section 5.1.10 Core Expertise)

5.2.14 **Senior Operations Subject Matter Expert (Non-Deployable) TS**

- Contractor shall:
- Demonstrate strong interpersonal skills and sufficient mastery of the IT profession to act as the Operations section lead training representative for both contractors and government personnel to include Cisco, Microsoft, and hardware troubleshooting disciplines.
- Demonstrate expertise in a broad range of technical skill sets tempered with confidence, leadership, and management capabilities to support the NOSC Director of Operations and Crew Commanders.
- Document processes and logic diagrams for regularly accomplished tasks on the NOSC operations floor as well as processes utilized by support technicians, typically referred to as Operations Knowledge Books.

- Develop technical documents such as TTPs, CONOPs and SPIN-C Tabs based on extensive networking background in system administration and network engineering.
- Research and analyze network topology via NOSC automated toolsets and a myriad of networking metrics to ascertain connectivity, topology, and status to recognize sub-standard network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Troubleshoot and utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.

- Utilize the Firewall toolset to accurately analyze and report on the overall health of local and deployed firewalls.
- Enterprise Level firewall fault isolation and correction to include troubleshooting ACLs affecting other network traffic.
- Perform local installation and local and remote administration of firewalls to include command line and GUI interfaces.
- Create, maintain and update a work schedule that provides 24/7 coverage for an IT tier two enterprise help desk.
- Develop and maintain training plans for all operations floor positions – mentor and educate operations personnel on new system installations and operating application upgrades.
- Act as the Director of Operations' liaison to provide critical information flow with all NOSC sections and senior military leadership.
- Possess and demonstrate a good understanding of geopolitical issues and interest related U.S. doctrine as applied to countries in the USAFCENT Area of Responsibility (AOR), Southwest Asia, especially in the areas for IT tier two enterprise help desk support.
- Stay current on technologies as applied to military and commercial Information Systems and Technologies to coordinate recommendations for both tactical and strategic planning purposes with USAFCENT/A6 and other senior staff.
- Provide oral and written briefs and presentations to senior IT managers explaining and support recommendations on IT tier two enterprise help desk support.
- Provide technical direction to other contractors for IT tier two enterprise help desk support.
- Mentor IT tier two enterprise help desk support staff for professional development and career progression to include both technical and managerial growth

5.2.14.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.14.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.14.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.14.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.14.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.2.14.6. Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.14.7. Installation Tasks (See Section 5.1.7 Core Expertise): Contractor shall provide direct or over-the-shoulder assistance as required using a variety of technologies as appropriate to the task.

5.2.14.8. Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents to explain abstract technologies and special interest items in easy to understand termination and examples. The Contractor shall also develop complex and complete tactics, techniques, and procedures (TTPs) on technologies and applications.

5.2.14.9. Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall provide technical support to other Subject Matter Experts/Engineers on a wide variety of technologies and applications.

5.2.14.10. Technical Certifications Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.2.15 Security Analyst (Non-Deployable) Secret (6)

- Conduct network security monitoring and intrusion detection analysis using the AFCENT/CENTCOM selected security tools to include but is not limited to IDS/IPS, firewall, proxy, router logs.
- Research Net Defense (NetD) to determine the necessity for deeper analysis and conduct an initial assessment of type and extent of intruder activates. Enter event data into mission support systems according to operational procedures and reports to meet AFCENT mission/tasking. The contractor shall produce a Suspicious Event Report (SER) for suspicious traffic meeting established thresholds.
- Track trends of authorized and unauthorized activity
- Correlate unusual and suspicious network activity across AFCENT. Validate unusual network activity unique to a geographical region and sensor location
- Provide an overall site-analysis profile to serve as a benchmark to identify unusual or suspicious activity
- Update incoming crews on the latest suspicious traffic identified during previous shift
- Provide focused NetD, tailored analysis and monitoring operations of specified sensor locations during contingency operations and in support of named NetD operations and exercises
- Assist in completion of NetD statistical and trend data and operational event reporting when requested
- Possess the following skill sets: extensive knowledge of network firewalls, computer and server log analysis, computer network servers (DNS, proxy, e-mail, domain controller, file server, Active Directory) and analysis of server logs.

- Maintain current knowledge on new vulnerabilities and exploits. Develop methods to detect and prevent intrusive activities utilizing knowledge. Assist NOSC-IA to develop countermeasures to isolate, contain and prevent intrusive actives and secure AFCENT/CENTCOM networks (to include IDS/IPS signature development and correlation rule sets)
- Track, document, and report all security related events including, but not limited to, Discharge of Classified Information and Cross Domain Violations IAW CENTCOM/AFCENT policy

- Coordinate and track Information Assurance Vulnerabilities Alerts (IAVA). Review and report AFCENT compliance to CENTCOM and develop Plans, Objectives, Actions and Milestones (POA&M) if unable to complete task.

5.2.15.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.15.2. LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.15.3. WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.2.15.4. OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.15.5. Network Security Tasks (See Section 5.1.6 Core Expertise)

5.2.15.6. Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents to explain abstract technologies and special interest items in easy to understand termination and examples. The Contractor shall also develop complex and complete tactics, techniques, and procedures (TTPs) on technologies and applications.

5.2.16 Computer Support Team (Non-Deployable) – SECRET

- Provide End User/Client level support to NOSC.
- Maintain and track NOSC End User/Client patch compliance
- Maintain and track NOSC Account Paperwork and Access

5.2.16.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.2.16.2. LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.2.16.3. OS Support Tasks (See Section 5.1.4 Core Expertise)

5.2.16.4. Network Security Tasks (See Section 5.1.6 Core Expertise)
5.2.16.5. Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents to explain abstract technologies and special interest items in easy to understand termination and examples. The Contractor shall also develop complex and complete tactics, techniques, and procedures (TTPs) on technologies and applications.

5.2.17 Information Technology Project Coordinator/Analyst Secret

Contractor shall:

- Have some Project Management background with specific experience with Microsoft Project and Project Server to manage network infrastructure, software development, and other information systems and technology projects.
- Assist in project plans, material acquisitions, time management, and detailed project action plans.
- Coordinate each new project with the project leads to customize the project plan to meet specific manning, time, and budget resources.
- Assist in project management oversight of information systems and technology projects from inception to completion.
- Manage and assist with coordination of IT contracts with GSA and Local Contracting offices for the acquisition of materials, equipment and services.
- Track project resources requests, Request for Quotes (RFQ), Request for Proposal (RFP), and Statements of Work (SOW).
- Install, configure, administer, and maintain Microsoft Project Server and other Web pages to provide access to project status, documentation, and related web-based products.
- Produce detailed professional reports, to brief status of projects to senior leaders, and provide statistical analysis for strategic planning and funding.

5.2.17.1 Project Plan Development Task: Contractor shall Assist project manager with the development of project plans showing assigned resources, materials required, estimated milestone dates, and other relevant details to each specific project. Contractor shall train NOSC personnel on the use and implementation of planning tools and on how to use these planning tools to better implement and track their projects. Contractor shall assist in capture project data and make it available via the web to all end users and local agencies. Contractor shall be familiarity with information systems and technology.

5.2.17.2 Project Resource Acquisition Task: Contractor will support the project manager in the management of acquisition resources (documentation, licensing, hardware, software, and other materials) required for each task through established funding procedures. Task involves compiling resource requirements from project engineers and assisting with converting those requirements into a purchase order requirements package. Contractor shall adhere to local procedures and regulations when purchasing said resources. Additionally, the project manager will compile project resources, manage storage of project resources, and coordinate shipment of project materials. All purchases will be reviewed, approved, and completed by Government representative prior to obligation and/or fulfillment.

5.2.17.3Web Based Applications and Servers Task: (See Section 5.1.5 Core Expertise) Contractor will contribute in maintaining a Project Management web page to access Microsoft Project Server and other Web pages to provide access to project status, documentation, and related web-based products. Contractor shall coordinate with the web development team for web server support.

5.2.17.4Documentation Task: Contractor shall document entire project in web format (soft copy available to all interested and applicable parties) and in archive format. Contractor shall coordinate the development of a file plan and implement the plan in order to archive all project related data for posterity and future reference. The file plan must conform to Air Force regulations and must include official archival, reviews, inspections, and proper classification markings in accordance with local and Air Force policy.

5.2.17.5Technical Coordinator Task: (See Section 5.1.9 Core Expertise): Contractor shall coordinate with internal and external agencies for the successful execution of project timeline elements. Coordination will include but is not limited to: Concept of Operations (CONOPS), Network Security Certifications, Country Clearance submissions and tracking, personnel movements, and project material acquisitions to include staging and buildup of equipment. Coordination will be documented in appropriate project software and maintained for historical and audit purposes.

5.2.17.6Technical Certifications Requirements (See Section 5.1.10 Core Expertise)
5.2.17.7Educational Requirements (See section 5.1.10 Core Expertise

5.2.18 Senior Cyber Assurance/Information Assurance Security Manager (ISSM) (Non-Deployable) TS/SCI

Contractor shall:

- Act as the primary cybersecurity technical advisor to the USAFCENT Authoring Official (AO)
- Recommended work strategies, pinpointing financial and quality areas of opportunity and recommend appropriate courses of action.
- Forecasted staffing needs and supported new hire selection and training process
- Assist in interpreting SPIN-C for individuals and leadership.
- Research, analyze, document and write systems security accreditation and certification requirement packages in accordance with applicable Air Force regulations and procedures; including documenting systems architecture and networks' physical layout in writing and graphical presentations.
- Analyze, evaluate, and recommend the application of Air Force systems accreditation and certification procedures in relation to existing and planned 9AF/USAFCENT network architecture at Shaw AFB and SWA.
- Research, Process, approve Firewall and Bluecoat Exception Request for implementation.
- Process request for RSSD, such as write to CD, USB for US and FFNs.
- Complete accreditation documents for USAFCENT as outlined by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Risk Management Framework (RMF), CENTCOM, and Authorizing Official (AO) guidance to include documenting systems architecture and physical network layout in writing and graphical presentations
- Maintain Enterprise Products List (EPL) and Accreditation Library for all approved products and systems and evaluate service level agreements.
- Assist with the completion of all accreditation documents for USAFCENT Cross Domain Solutions as outlined IAW DoD and CENTCOM regulations
- Research, analyze, and document AFCENT Information Assurance and Security polices IAW DISA, CENTCOM, and USAF regulations and guidance.
- Track, document, and report all security related events including, but not limited to, Discharge of Classified Information and Cross Domain Violations IAW CENTCOM/AFCENT policy

- Coordinate and track Information Assurance Vulnerabilities Alerts (IAVA). Review and report AFCENT compliance to CENTCOM and develop Plans, Objectives, Actions and Milestones (POA&M) if unable to complete task.

- Coordinate and track Information Assurance Vulnerabilities Alerts (IAVA). Review and report AFCENT compliance to CENTCOM and develop Plans, Objectives, Actions and Milestones (POA&M) if unable to complete task.

Manage and mentor Cyber Policies and Research and Cyber Network/Systems Certification and Accreditation-RMF technicians for professional development and career progression to include both technical and managerial growth.

5.2.18.1 General Networking Tasks (See Section 5.1.1 Core Expertise)
5.2.18.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)
5.2.18.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)
5.2.18.4 OS Support Tasks (See Section 5.1.4 Core Expertise)
5.2.18.5 Network Security Tasks (See Section 5.1.6 Core Expertise
5.2.18.6 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.
5.2.18.7 Documentation Task (See Section 5.1.8 Core Expertise)
5.2.18.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise)
5.2.18.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3 USAFCENT Network Deployable Support Tasks

5.3.1 Senior Network/Systems Security Accreditation and Technical Writing/Documentation (Deployable) - TS

- Contractor shall:
- Develop technical documents based on extensive networking background in system administration or network engineering.
- Complete accreditation documents for USAFCENT systems and networks using USAF Network Security and Accreditation instructions and guidance for System Security Authorization Agreement as outlined by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Risk Management Framework (RMF).
- Research, analyze, document and write systems security accreditation and certification requirement packages in accordance with applicable Air Force regulations and procedures; including documenting systems architecture and networks' physical layout in writing and graphical presentations.
- Analyze, evaluate, and recommend the application of Air Force systems accreditation and certification procedures in relation to existing and planned 9AF/USAFCENT network architecture at Shaw AFB and SWA.
- Use experience with network architecture and design to predict possible impact of installing new software and hardware in an existing network enterprise.

- Research network topology via NOSC automated toolset (Openview, etc) to ascertain connectivity, topology, and status to document processes and logic diagrams for regularly accomplished tasks on the NOSC operations floor as well as processes utilized by support technicians, typically referred to as Knowledge Books.
- Develop and manage all phases of the documentation project(s) including initial analysis, information gathering, design of deliverables, and distribution of finished product.
- Provide for all security test and evaluation requirements to determine network vulnerabilities associated with final network accreditation, to include team management, fact gathering, testing, evaluation, and documentation.
- Assist other government and contracted personnel with project documentation and web site development as needed.
- Assist the Training Manager with standardization and transcription of training materials.

- Complete accreditation documents for USAFCENT as outlined by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Risk Management Framework (RMF), CENTCOM, and Authorizing Official (AO) guidance to include documenting systems architecture and physical network layout in writing and graphical presentations
- Maintain Enterprise Products List (EPL) and Accreditation Library for all approved products and systems
- Complete accreditation documents for USAFCENT Cross Domain Solutions as outlined IAW DoD and CENTCOM regulations
- Research, analyze, and document AFCENT Information Assurance and Security polices IAW DISA, CENTCOM, and USAF regulations and guidance

5.3.1.1. General Networking Tasks (See Section 5.1.1 Core Expertise): Contractor shall maintain a standard set of published network architectural diagrams; establish and coordinate periodic reviews and publishing to keep information accurate for use by Network Engineers and Helpdesk Technicians. Ensure Enterprise and Site network architecture drawings and diagrams are up to date and accurate. Establish and maintain a web page to provide deployed sites up/download access for site-specific drawings and diagrams.

5.3.1.2. LAN Support Tasks (See Section 5.1.2 Core Expertise): Contractor shall understand the use of Dynamic Host Control Protocol (DHCP), Windows Internet Naming Service (WINS), Dynamic and Integrated Domain Name Service (DNS), and Active Directory (AD) principles and integrate these technologies into standard technical references.

5.3.1.3. WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise): Contractor shall develop logic flow charts for Enterprise processes utilized by the NOSC and deployed sites. Provide standardized written procedures and/or checklists for associated with common tasks and procedures.

5.3.1.4. OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.1.5. Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.1.6. Network Security Tasks (See Section 5.1.6 Core Expertise): Contractor shall document, create, maintain, and track network accreditation packages throughout their life cycle for local and deployed networks. Visit each site annually or sooner if required to maintain site network accreditation. Work with the Web Design Engineer and Programmer to provide access to the accreditation documentation using standard NOSC web page design practices.

5.3.1.7. Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.1.8. Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall transfer rough draft technical documentation into a standard document format for formal publishing. Work with Network Engineers and Project Leads to document Concept of Operations, Engineering Plans, and Tactics, Techniques and Procedures (TTPs). Establishes and coordinates an annual review of published documentation. Develop logic flow charts for processes utilized by the NOSC and deployed sites. Provide standardized written procedures and/or checklists for associated with common tasks and procedures. Function as lead reviewer and coordinates a semi-annual review of the Special Instructions for Communicators (SPIN-C). Write the System Security Authorization Agreement appendix for NOSC network projects in support of the NOSC and SWA.

5.3.1.9. Technical Coordinator (See Section 5.1.9 Core Expertise): Contractor shall aid Training Manager by standardizing training material. Review ITSM trouble tickets and create a knowledge base utilized by the level help desk technicians for fault isolation and resolution.

5.3.1.10. Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.1.11. Educational Requirements (See Section 5.1.10 Core Expertise)

5.3.2 Network Security Analysis (Deployable) – TS/SCI

Contractor shall:

- Build tactical and strategic network profiles of specific systems and complete network architecture.
- Analyze network intrusion detection systems and conduct vulnerability assessments.
- Develop system concept of operations and engineering plans to execute security requirements for new and existing systems with a focus on incident response policies and procedures.
- Develop reports and trend analysis documentation on bandwidth, network architecture, as well as network security incidents.
- Utilize operational knowledge of network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools includes Internet Security Scanner (ISS), Cisco Security Agent (CSA), SecureWave, and other zero-day personal firewall and security agents.
- Implement a variety of virtual private network (VPNs) both software (IPSec) and hardware solutions.
- Provide on-shift training representative for both contractors and government personnel to include CISCO, Microsoft, hardware, and vulnerability assessment and troubleshooting.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Provide crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Attend daily Theater Network Control Central Cyber Defense briefings.

- Facilitate weekly Information Assurance telecons.
- Provide guidance on basic Information Assurance policy
- Provide organizational e-mail monitoring

5.3.2.1 **Advanced Traffic Analysis Task**

- Validate unusual network activity unique to a geographical regions and sensor locations
- Provide an overall site-analysis profile to serve as a benchmark to identify unusual or suspicious activity
- Possess the following skill sets: extensive knowledge of network firewalls, computer and server log analysis computer network servers (DNS, proxy, e-mail, domain controller, file server, Active Directory) and analysis of their logs
- Provide technical assistance in the planning, testing, development, implementation, enhancement, transition, management and operations of new AFCENT initiatives and support the integration of these systems into existing architecture
- Analyze live and historical data for events related to possible network infiltration

- Maintain current knowledge on new vulnerabilities and exploits. Develop countermeasures (to include IDS/IPS signature development and correlation rule sets) to isolate, contain and prevent intrusive actives and secure AFCENT/CENTCOM networks
- Develop methods to identify contain, log, and analyze intrusive activities and security vulnerabilities on AFCENT networks

5.3.2.2 **Incident Response Analysis Task**

- Perform network traffic and host analysis to evaluate intruder activities using host and network based monitoring system. Correlate information gathered to provide effective methods to protect the AFCENT domain. Ensure appropriate notification action is taken to reduce the risk to the AFCENT networks.
- Conduct network and computer forensics on suspected and confirmed compromised system to determine the method of intrusion and corrective actions to be taken to prevent or detect similar future activities.
- Develop methods to identify contain, log, and analyze intrusive activities and security vulnerabilities on AFCENT networks. Prevent intruders from accessing AFCETN resources. Maintain current knowledge on new vulnerabilities and exploits. Develop countermeasures (to include IDS/IPS signature development and correlation rule sets) to isolate, contain and prevent intrusive actives and secure AFCENT/CENTCOM networks
- Maintain current knowledge on existing and new malware behavior and propagation characteristics. Maintain current knowledge on the anti-virus tools currently in use by AFCENT/CENTCOM. Develop methods to identify, contain, log, and analyze malware-based activities on AFCENT networks

5.3.2.3 **Vulnerability Analysis Task:**

- Utilize DoD mandated vulnerability scanner to scan for vulnerabilities on the AFCENT enterprise
- Assist in providing reports and metrics as required by active duty, government civilians, and contractors
- Track AFCENT vulnerability and patch compliance and provide trending analysis

5.3.2.4 Security Device Maintenance Tasks

- Install, configure, maintain, and manage the AFCENT/CENTCOM security devices to include but is not limited to IDS/IPS, ArcSight Enterprise Security Manager, ACAS and associated Virtual Private Network (VPN) equipment/configurations. Assist in development and documentation of sensor process and checklists.
- Support CENTCOM operations by providing the capability to “omit” or filter sensor traffic and alerts reporting activity based on AFCENT NOSC-IA’s instruction that traffic does not need to be reviewed in a “real-time” operation by analysts

- Provide technical advice and assistance to the AFCENT NOSC-IA to resolve network issues and perform actions necessary to ensure IDS/IPS sensors are collecting and reporting network activity. Diagnose and resolve end user problems. Ensure the end users adhere to the proper security policies and procedures.
- Conduct troubleshooting and fault isolation to ensure network connectivity to the sensor equipment. Establish VPNs between AF and CENTCOM sites for protected communications. Maintain commercial off the shelf (COTS) and access control lists to restrict unauthorized access to network resources

5.3.2.5 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.2.6 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.2.7 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.2.8 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.2.9 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.2.6 Network Security Tasks: Contractor shall manage and maintain control of network intrusion detection systems (IDS). Ensure end-to-end operations for network and information technology systems.

Security: Contractor shall monitor network traffic to determine system vulnerabilities and required fixes; apply established network security procedures, logs and makes recommendation for correcting network security incidents; coordinate the escalation of security issues requiring detailed analysis to Security Analyst.

Intrusion Detections: Contractor shall examine logs and information gained from network sniffers or protocol analyzers to determine if possible outside or unauthorized access has occurred. Track and record possible intrusion or security breach from routine daily analysis for successful anomaly/intrusion identification, including writing detailed analysis for legal use. Contractor may be required to provide oral or written findings and explanation of events for any legal actions associated with security breaches.

Vulnerability Assessment: Contractor shall use vulnerability toolset to determine networks and systems security weaknesses and shortfalls. Research and coordinate vulnerability finding with Security Analysis to provide detailed fix actions. Coordinate with other computer emergency response team (CERT) to ensure latest known vulnerabilities are properly identified and corrected.

5.3.2.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.2.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.2.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.2.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.3 Network Security (Deployable) TS/SCI

- Contractor shall:
- Utilize experience and knowledge to analyze network intrusion detection systems and conduct vulnerability assessments.
- Develop reports and trend analysis documentation on bandwidth, network architecture, as well as network security incidents.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.

- Use advanced technical writing skills to develop and update IT systems concept of operations and engineering plans.
- Create and manage network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to include Certification Authority (CA) and a variety of virtual private network (VPNs) both software and hardware.
- Analyze live channel data for events related to possible network breeches
- Create computer network defense reports on events of concern
- Monitor and track events until resolution is obtained
    - Master block list monitoring
    - Network defense action monitoring
    - Network investigation actions
- Provide Counter Access Team support
    - Perform deep dive incident analysis to include determining impact and executing containment and cleanup actions

- Identify previously undetectable malware and reverse engineer
- Search for the unknown or advanced persistent threat

- Identify and remove any potentially harmful unauthorized software

5.3.3.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.3.2 LAN Support Tasks (See Section 5.1.2 Core Expertise): Contractor shall research, document, and track to resolution all outages, trouble calls, and network intrusions. Utilize the Firewall toolset to accurately analyze and report on the overall health of local and deployed firewalls. Recommend appropriate changes/resolutions in response to the trends analysis. Enterprise Level firewall fault isolation and correction to include troubleshooting ACLs and Proxies affecting other network traffic. Provide On-the-job training to local help desk personnel and engineers on firewall components and solutions. Configures and maintains DNS and BIND domain name services and manage the full range of Sidewinder features at an Enterprise level.

5.3.3.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise): Contractor shall provide guidance and remote administration in the following areas related to Sidewinder and the Enterprise Manager (EM):

a. General Optimization
b. VPN connections between firewalls (Point to Point)
c. ACL management
d. IP Filter management
e. Log analysis
f. Installation
g. Cloning
h. One-to-many – Failover

5.3.3.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.3.5 Open Secure-BSD OS: Contractor shall troubleshoot firewall issues on Open BSD Operating System, including permissions and type-enforcement. Contractor shall follow proper backup procedures to walk remote users through successful backups and restoration actions, and accomplish the same locally.

5.3.3.6 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.3.7 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.3.8 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.3.9 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.3.10 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.3.11 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.4 Network Firewall Security (Deployable) – Secret

Contractor shall:

- Troubleshoot and develop solutions for anomalies both remotely and locally for security devices to include but not limited to HBSS, Firewalls, and Logging Solution's.
- Analyze firewall reports, firewall logs, and other metrics and identify sub-standard network performance. Engineer solutions and implement improvements to counter the identified anomalies.
- Develop reports and trend analysis documentation on bandwidth and network security incidents and brief recommendation to senior staff.
- Operate security devices remotely and locally via command line and GUI interface when applicable.
- Operate and manage the Enterprise Manager, ensuring it is functional with duplicate configuration on an off-line EM.
- Create VPN certificates and manage VPN Gateways for deploying remote users.
- Use strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Sidewinder Software, VPN management, report analysis, and hardware troubleshooting disciplines.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent security device outages/problems/issues..
- Direct, organize, and utilize crisis management techniques during outages and in high-pressure environments.
- Use mastery of UNIX scripting to create custom scripts to meet task specific requirements
- Monitor health of HBSS and maintain configuration per DISA/CENTCOM direction
- Assist engineering new security device implementations

5.3.4.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.4.2 LAN Support Tasks (See Section 5.1.2 Core Expertise): Contractor shall research, document, and track to resolution all outages, trouble calls, and network intrusions. Utilize the Firewall toolset to accurately analyze and report on the overall health of local and deployed firewalls. Recommend appropriate changes/resolutions in response to the trends analysis. Enterprise Level firewall fault isolation and correction to include troubleshooting ACLs and Proxies affecting other network traffic. Provide On-the-job training to local help desk personnel and engineers on firewall components and solutions. Configures and maintains DNS and BIND domain name services and manage the full range of Sidewinder features at an Enterprise level.

5.3.4.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise): Contractor shall provide guidance and remote administration in the following areas related to Sidewinder and the Enterprise Manager (EM):

a. General Optimization
b. VPN connections between firewalls (Point to Point)
c. ACL management
d. IP Filter management
e. Log analysis
f. Installation
g. Cloning
h. One-to-many – Failover

5.3.4.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.4.5 Open Secure-BSD OS: Contractor shall troubleshoot firewall issues on Open BSD Operating System, including permissions and type-enforcement. Contractor shall follow proper backup procedures to walk remote users through successful backups and restoration actions, and accomplish the same locally.

5.3.4.6 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.4.7 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.4.8 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.4.9 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.4.10 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.4.11 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.5 Senior Network/Systems Training and Curricular Development (Deployable) Secret

- Contractor shall:
- Provide sourcing, scheduling, and documenting training. Contractor shall be required to conduct training. The trainer will develop new curriculum to meet current and future training requirements from scratch.
- Supervise other training managers to include scheduling their work to support approved training requirements.
- Develop training plans, training aids, and training records for networking professionals.
- Primary duties include training deploying personnel, writing lesson plans and training material, maintaining the training facility and associated lab equipment to include setup

and tear down for each class, maintaining web-base scheduling and training materials, and teaching reoccurring training courses to NOSC personnel and other contractors.

- Establish training programs to meet local knowledge and skill requirements and to enhance professional awareness of the technologies utilized in the NOSC work center as well as at deployed Network Control Center locations.
- Contractor shall develop portable training materials to be delivered over multiple media, including traditional classroom, web-based, and CD-ROM based training.

5.3.5.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.5.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.5.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.5.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.5.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.5.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.5.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.5.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.5.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.5.10 Training Development Task: Contractor shall develop training lesson plans and accompanying educational materials. Train NOSC and deploying personnel on current software and equipment used by the NOSC and at deployed locations. Training includes, but not limited to, Microsoft, Sun, HP, Cisco, and Linux OS. Training also requires familiarity with applicable/associated hardware for Sun, CISCO, ODS, and various x86 processor based servers equipment. Training for new technologies will be provided by the government and the Senior Network/System Training Curricular Development SME must be capable of translating/tailoring the training for the use of the NOSC-D. Training development requires traditional training materials to be converted to web or CD-ROM base media on an as required basis.

5.3.5.11 Formal Training Facility Task: Contractor shall manage the training room/facility, and associated lab, including the training servers and student PC. Identify necessary equipment

and materials necessary to accomplish/meet the training objectives. Maintain an automated scheduling database for the training lab.

5.3.5.12 Training Management Task: Contractor shall source a wide variety of LAN/WAN training courses from both Air Force and commercial training sites in support of USAFCENT mission; schedule personnel for training courses; develop in-house training classes/seminars; schedule and conduct in-house networking technology training classes; conduct and facilitate On-the-Job Training; evaluate, analyze, and document critical work center tasks; develop work center training plan in accordance with applicable Air Force training standards, instructions, and regulations; track and document employees training progression; certify employees ability to perform tasks. Assess the applicability of commercial training to be integrated in to the NOSC-D training plan.

5.3.5.13 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.5.14 Educational Requirements (See Section 5.1.10 Core Expertise)

5.3.6 Network Architecture Design Engineer Subject Matter Expert (Deployable) Secret

- Contractor shall:
- Use extensive LAN/WAN background with designing External Gateway Protocol (EGP) such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and Interior Gateway Protocol (IGP) such as and Enhanced Interior Gateway Routing Protocol (EIGRP).
- Troubleshoot and develop solutions for network anomalies both remotely and locally. Analyze a myriad of networking metrics and recognize sub-par network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Troubleshoot network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to ensure proper design and integration;
- Administer advanced Cisco network products such as VoIP and other advanced technologies.

- Posses strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco Switches and Routers, and hardware troubleshooting disciplines; who has a solid working knowledge of basic LAN technologies and OS used on deployed networks.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues. Must direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of skill sets tempered with confidence and leadership the Contractor shall be expected to function with minimal supervision.

5.3.6.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.6.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.6.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.6.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.6.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.6.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.6.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.6.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.6.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.6.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.7 Enterprise Messaging Systems (Deployable) Secret
k

- Contractor shall:
- Provide support for Microsoft Exchange (2010 and later).
- Manage e-mail capability of using signed and encrypted technology associated with encryption devices High Grade Service (HGS) and Public Key Infrastructure (PKI) Medium Grade Service (MGS).
- Use technical writing skills to develop and maintain system concept of operations (CONOPS), engineering plans, and user guides for AMHS.

- Analyze a wide array of system performance metrics to recognize substandard performance. Troubleshoots and develops viable options to resolve substandard performance anomalies both remotely and locally.
- Develop reports and trend analysis documentation on system use to include account utilization, Directory Information Tree (DIT) accuracy, mail flow delivery, directory replication, and Global Address List (GAL) replications using Microsoft Metadirectory Service (MMS) and/or Microsoft Identity Information Server (MIIS) with the AF Hub.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.

- Provide for crisis management during outages, virus outbreaks, and in high-pressure environments. Contractor shall possess a broad range of expertise in Commercial Electronic mail technologies.

5.3.7.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.7.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.7.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.7.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.7.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.7.6 Network Security Tasks (See Section 5.1.6 Core Expertise): Contractor shall coordinate with the firewall administrators to ensure proper access control lists (ACL) and Internet Protocol (IP) filters are in place for network protection and security.

5.3.7.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.7.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.7.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise):

5.3.7.10 X509 User Request Forms Creation and Management Task : Contractor shall coordinate with the Regional Certificate Authority Workstation (CAW), Deployed Responsible Officer (FRO) and users to define requirements to establish AMHS accounts. Validate, complete, submit, ship, and track encryption cards to their deployed locations. Ensure the accounts are properly configured and maintained in the Directory Information Tree (DIT).

5.3.7.11 Administrator Directory User Agent (ADUA) Task: Contractor shall use the Administrator Directory User Agent to maintain USAFCENT Deployed force AMHS accounts in the Directory Information Tree (DIT). Create, modify, and delete accounts as required to comply with DoD, AF, and USCENTF directives.

5.3.7.12 Plain Language Address (PLA) and Address Indictor Group (AIG) Task: Contractor shall coordinate the Plain Language Address (PLA) and Address Indictor Group (AIG) controlling authority to ensure PLA are proper associated with specific AMHS accounts. Contractor shall submit and monitor AIG and (Distribution Lists) for USAFCENT AMHS accounts. Provide deployed users with necessary training to ensure continuity of operations are maintained at deployed locations.

5.3.7.13 Global Address List (GAL) Task: Contractor shall monitor the transfer of Global Address information between the USAFCENT enterprise and the AF enterprise. Ensuring replication of the USAFCENT enterprise operational is and available for export and exchange. Maintain a web-centric GAL data exchange website for components not capable of using Microsoft Metadirectory Service. Ensure manually imported and exported data current to within 30 days.

5.3.7.14 Public Key Infrastructure (PKI) Management Task: Contractor shall coordinate and provide direction to user on the implementation of the PKI at the user level. Validate user certificates associated with Commercial Exchange accounts were properly stored in the GAL. Work with deployed locations to maintain a stock of PKI soft-tokens for use until the full implementation of the Common Access Card (CAC) is successful in the USAFCENT AOR. Coordinate with other USAFCENT components to ensure USAFCENT forces receiving e-mail support from other components are capable of using PKI successfully.

5.3.7.15 Automated Messaging Handling Systems (AMHS) Task: Contractor shall provide expertise for X.400, X500/ Lightweight Directory Access Protocol (LDAP), and Simple Mail Transfer Protocol (SMTP) e-mail protocols. Maintain the messaging service between AMHS and the Commercial Exchange servers including X.400 and X.509 certificates interoperability. The Contractor shall ensure operation of primary and secondary systems, and failover at the alternate NOSC location, and maintain the user web site providing user access request.

5.3.7.16 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.8 Network System Design (Deployable) Secret

- Contractor shall:
- Analyze a wide array of networking metrics and recognize substandard network performance.
- Troubleshoot and develop solutions for network anomalies both remotely and locally.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.

- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Provide for crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Create and manage network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to include Certification Authority (CA) and a variety of virtual private network (VPNs) both software and hardware .
- Use advanced technical writing skills to develop and update IT systems concept of operations and engineering plans.

5.3.8.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.8.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.8.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.8.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.8.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.8.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.8.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.8.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.8.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.8.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.9 Information Technology Systems (Deployable) Secret

- Contractor shall:
- Use common patch management tools such as Microsoft System Control Center Manager (SCCM), System Update Server (SUS), Microsoft Security Baseline Analyzer (MSBA), and vulnerability detection tools and utilities.
- Troubleshoot and develop solutions for IT systems and network anomalies both remotely and locally.
- Develop reports and trend analysis documentation on IT systems bandwidth requirements and security incidents.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.

- Direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Use advanced technical writing skills to develop and update IT systems concept of operations and engineering plans.
- Create and manage network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to include Certification Authority (CA) and a variety of virtual private network (VPNs) both software and hardware.

5.3.9.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.9.2 LAN Support Tasks (See Section 5.1.2 Core Expertise): Contractor shall develop user guidance documents and installation instructions. Develop and implement an active directory architecture solution. Test and validate IT systems security patches and hot-fixes as defined by Information Assurance Vulnerability Alerts (IAVA), Time Compliance Network Orders (TCNO), and local security guidance. Support the distribution of security patches throughout the enterprise using Microsoft Systems Management Server (SMS), System Update Server (SUS), Microsoft Security Baseline Analyzer (MSBA), and other enterprise level tools. Provide configuration management for the SMS distributed enterprise architecture. Provide support and instructions to remote locals using telephone, on-site visits, and terminal services. Use data replication software to keep sites up-to-date with software packages and other software. Track package deployment and status updates using on-line trouble ticketing (Remedy) systems.

5.3.9.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.9.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.9.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise): Contractor shall work with the Web Development team to maintains the SMS web page. The SMS Web will provide deployed members with easy access to Patches, Meeting minutes, TTPs, and other SMS related documentation.

5.3.9.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.9.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.9.8 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall coordinate with Information Assurance to document the current patch-level of all PCs, servers, and network devices identified in IAVA and TCNOs. Status display and documentation will include graphs, charts, and tables. Develop, design, create, write, and modify SMS queries, collections, packages, and advertisements to distribute enterprise level security patches, hot-fixes, and other software as required.

5.3.9.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall coordinate the dissemination of security vulnerabilities using the Communications Tasking Order (CTO) to deployed sites.

5.3.9.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.10 Network Modeling and Simulation (Deployable) Secret

- Contractor shall:

- Develop network models from existing network architectures using collected network management data for the purpose of running simulations to analyze a myriad of networking metrics and recognize sub-standard network performance.
- Resolve, improve, or prevent network problems/issues.
- Provide for crisis management during outages, virus outbreaks, and in high-pressure environments.
- Manage and configure advanced network management toolset to collect data to build a Network Common Operational Picture (NETCOP).
- Develop and update IT systems concept of operations and engineering plans.

5.3.10.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.10.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.10.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise): Contractor shall research and design wide area networks either as new networks or to modify existing networks. Design and implementation must be fully documented with engineering plans to detail the complete process from inception to activation. Recommend appropriate changes/resolutions in response to tactical and strategic trend analysis derived from network and systems models.

5.3.10.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.10.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.10.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.10.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.10.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.10.9 Network Engineering Task: Contractor shall understand where different operating systems are used, and can explain the advantages and disadvantages of each. Applies System Development Life Cycle (SDLC) principles associated with new and upgrade requirements.

5.3.10.10 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall research cutting edge technologies to determine applicability to the USAFCENT data-networking mission. Contractor shall be the primary point of contact for technical coordination with technology vendors for using commercial-off-the-shelve (COTS) technology, and custom designed and engineered solutions specific to the USAFCENT. However, the Contractor shall not negotiate with vendors on changes or new requirements that could obligate the government, or incur charges.

5.3.10.11 Briefing and Presentation Task: Contractor shall use Microsoft Power Point to prepare briefing and presentations in support of Network Modeling and Support tasks. Contractor shall deliver briefings to the USAFCENT/A6 and other senior staff on an as required basis, and will typically include pre and post symposium and conference briefing. Briefing will be provided in both oral and written formats. Contractor shall assist the Chief of NOSC Engineering Support Team (NEST) to provide technical and status updates to the NOSC commander on a weekly basis. Contractor shall independently brief Modeling and Simulation project and production issues with little or no-notice.

5.3.10.12 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.10.13 Educational Requirements (See Section 5.1.10 Core Expertise)

5.3.11 Senior Systems Analysis (Deployable) – TS/SCI

- Contractor shall:
- Possess and demonstrate a good understanding of geopolitical issues and interest related U.S. doctrine as applied to countries in the USAFCENT Area of Responsibility (AOR), Southwest Asia, especially in the areas of IT.
- Stay current on technologies as applied to military and commercial Information Systems and Technologies to coordinate recommendations for both tactical and strategic planning purposes with USAFCENT/A6 and other senior staff on IT subjects.
- Provide oral and written briefs and presentations to senior IT managers explaining and support recommendations.
- Maintain a professional image and appearance, including appropriate attire commensurate with this senior staff position. Profession business attire will be commensurate with government uniforms, and other contractor attire.
- Provide technical direction to other contractors on network and systems engineering to develop network and systems engineering concepts and apply System Development Life Cycle (SDLC) principles.
- Provide technical coordination and research to exploit cutting-edge technologies, assisting with technical and status updates for briefings and reporting.
- Mentor other NOSC engineers for professional development and career progression to include both technical and managerial growth.
- Review technical project documentation for final draft coordination and subsequent release. Includes assisting personnel with project documentation and web site development as needed.
- Coordinate technical visits from Air Force and other military agencies, and Contractors.

5.3.11.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.11.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.11.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.11.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.11.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.11.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.11.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.11.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.11.9 Network Engineering Task: Understands where different operating systems are used, and can explain the advantages and disadvantages of each. Can apply System Development Life Cycle (SDLC) principles associated with all the above.

5.3.11.10 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall research cutting edge technologies to determine applicability to the USAFCENT data-networking mission. Contractor shall be primary point of contact with technology vendors for using commercial-off-the-shelve (COTS) technology, and custom designed and engineered solutions specific to the USAFCENT. However, the Contractor shall not negotiate with vendors on changes or new requirements that could obligate the government, or incur charges.

5.3.11.11 Briefing and Presentation Task: Contractor shall use Microsoft Power Point to prepare briefings and presentations in support of IT initiatives. Briefing will be delivered to the USAFCENT/A6 and other senior staff on an as required basis, and will typically include pre and post symposium and conference briefing. Briefing will be provided in both oral and written formats. Contractor shall assist the Chief of NOSC Engineering Support Team (NEST) to provide technical and status updates to the NOSC commander on a weekly basis. Contractor must be prepared to brief all NEST project and production issues with little or no-notice.

5.3.11.12 Mentoring and Profession Development Task: Contractor shall support military and contractor data and systems engineers offering technical and management experience with project management and development. This includes assisting with the writing of Concept of Operations, Engineering Plans, Special Instructions for Communicators (SINC), and other technical documentation. Assists Project Leads with determining project scope, timelines, list of materials, coordination meetings, and general project management as required.

5.3.11.13 Technical Project Review Task: Contractor shall review final draft of all technical documentation for both data and systems projects. "Final-Draft" documents will be submitted for inclusion with other project documentation for final coordination.

5.3.11.14 Coordination and Liaison Task: Contractor shall coordinate visits from Air Force, other military agencies, and Contractors. Contractor shall coordinate the schedule to prevent conflicts with other projects and schedules and to maximize effectiveness of visits and use of resources. Contractor shall coordinate the need to allocate NOSC resources with senior staff.

5.3.11.15 Trip Reporting Documentation Task: All trip reports will be full documented and are due within five duty days of return. Trip reports will be provided for all Conferences, Seminars, In-Progress Reviews, Technical Development and Engineering Studies. Trip reports will be in standard AF format and delivered to the Chief of NOSC Engineering Support for review.

5.3.11.16 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.11.17 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.12 Senior Network Security (Deployable) – TS/SCI

- Contractor shall:
- Build tactical and strategic network profiles of specific systems and complete network architecture utilizing extensive LAN/WAN expertise.
- Analyze network intrusion detection systems and conduct vulnerability assessments.
- Develop system concept of operations and engineering plans to execute security requirements for new and existing systems with a focus on incident response policies and procedures.
- Develop reports and trend analysis documentation on bandwidth, network architecture, as well as network security incidents.
- Demonstrate operational knowledge of network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools includes Internet Security Scanner (ISS), Cisco Security Agent (CSA), SecureWave, and other zero-day personal firewall and security agents.
- Implement a variety of virtual private network (VPNs) both software (IPSec) and hardware solutions.

- Provide on-shift training representative for both contractors and government personnel to include CISCO, Microsoft, hardware, and vulnerability assessment and troubleshooting.
- Contractor shall make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments, demonstrates expertise in a broad range of skill sets tempered with confidence and leadership.

5.3.12.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.12.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.12.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.12.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.12.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.12.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.12.7 Intrusion Detections Task: Contractor shall examine logs and information gained from network sniffers or protocol analyzers to determine if possible outside or unauthorized access has occurred. Track and record possible intrusion or security breach from routine daily analysis to successful anomaly/intrusion identification, includes writing detailed analysis for legal use. Contractor shall function as government subject matter security expert for any legal actions associated with security breaches.

5.3.12.8 Vulnerability Assessment Task: Contractor shall use vulnerability toolset to analyze networks and operation systems to determine security weaknesses and shortfalls. Research and provide detailed fix actions for all identified vulnerabilities. Coordinate with other computer emergency response team (CERT) to ensure latest known vulnerabilities are properly identified and corrected.

5.3.12.9 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.12.10 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.12.11 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.12.12 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.13 Senior Network Architecture and Design (Deployable) – TS

- Contractor shall:
- Design External Gateway Protocol (EGP) such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and Interior Gateway Protocol (IGP) such as and Enhanced Interior Gateway Routing Protocol (EIGRP).
- Troubleshoot and develop solutions for network anomalies both remotely and locally. Analyze a myriad of networking metrics and recognize sub-par network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Troubleshoot network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to ensure proper design and integration.
- Administer advanced Cisco network products such as VoIP and other advanced technologies.
- Contractor shall act as an on-shift training representative for both contractors and government personnel to include Cisco Switches and Routers, and hardware troubleshooting disciplines, LAN technologies and OS used on deployed networks.
- Make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues. Contractor shall direct, organize, and utilize crisis management techniques during outages, and virus outbreaks in high-pressure environments.
- The Contractor shall be expected to function with minimal supervision.

5.3.13.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.13.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.13.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.13.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.13.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.13.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.13.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.13.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.13.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.13.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.14 Senior Network Systems Design (Deployable) – TS

- Contractor shall:
- Analyze a wide array of networking metrics and recognize substandard network performance.
- Troubleshoot and develop solutions for network anomalies both remotely and locally.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Direct, organize, and utilize crisis management techniques during outages, and virus outbreaks in high-pressure environments.
- Create and manage network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to include Certification Authority (CA) and a variety of virtual private network (VPNs) both software and hardware .
- Develop and update IT systems concept of operations and engineering plans.

5.3.14.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.14.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.14.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.14.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.14.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.14.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.14.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.14.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.14.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.14.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.14.11 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.15 IT Standards Assurance (Deployable) Secret

- Contractor shall:
- Develop technical documents based on extensive networking background in system administration or network engineering.
- Coordinate the NOSC participation in NOSC Process validation exercises such as Black Demon Exercises, acting as the primary focal point for all phases of the exercise.
- Conduct periods Personnel Evaluation based on Job Qualifications Standards as signed off in personnel Training Records (623) to determine the effectiveness of Initial Training, need for Supplemental Training, need for enhanced Proficiency Training, for the need for Recertification Training if standards not are not met,
- Coordinate closely with Training Managers to monitors inside and outside Certifications Evaluations, to enhance the overall quality and optimize training retention.
- Coordinate semi-annual site Staff Assistance Visits (SAV), or provides on-demand SAV at the request of deployed Senior Communications (SC); SAV augmentation may come from AFCA ScopeEdge, or internal NOSC resources.
- Review standard systems and network processes and checklist to validate they meet prescribed standards, and are easily executed from a comprehensive checklist.
- Coordinate on the development of training materials to ensure they meet Joint, CENTCOM, AFCENT, and AF standards for NOSC operations.
- Assist the Training Manager to develop/modify standardized training to meeting NOSC mission requirements.

5.3.15.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.15.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.15.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.15.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.15.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.15.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.15.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.15.8 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall produce written reports defining each inspection/evaluation to include, processes, procedures, findings, and recommendation. Due to the sensitivity of the reports they will only be reviewed by the NOSC Commander, appropriate section-head, or the individual themselves. Documents will be safeguarded in accordance with Privacy Act directives.

5.3.15.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall coordinate all evaluations with the appropriate section-head. Section-head will determine time and date of evaluations based on operational tempo and availability of personnel.

5.3.15.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.16 Senior IT Standards Assurance (Deployable) TS

- Contractor shall:
- Develop technical documents based on extensive networking background in system administration or network engineering.
- Coordinate the NOSC participation in NOSC Process validation exercises such as Black Demon Exercises, acting as the primary focal point for all phases of the exercise.
- Conduct periods Personnel Evaluation based on Job Qualifications Standards as signed off in personnel Training Records (623) to determine the effectiveness of Initial Training, need for Supplemental Training, need for enhanced Proficiency Training, and the need for Recertification Training if standards not are not met,
- Coordinate closely with Training Managers to monitors inside and outside Certifications Evaluations, to enhance the overall quality and optimize training retention.
- Coordinate semi-annual site Staff Assistance Visits (SAV), or provides on-demand SAV at the request of deployed Senior Communications (SC); SAV augmentation may come from AFCA ScopeEdge, or internal NOSC resources.
- Review standard systems and network processes and checklist to validate they meet prescribed standards, and are easily executed from a comprehensive checklist.
- Coordinate on the development of training materials to ensure they meet Joint, CENTCOM, AFCENT, and AF standards for NOSC operations.
- Assists the Training Manager to develop/modify standardized training to meeting NOSC mission requirements.

5.3.16.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.16.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.16.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.16.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.16.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.16.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.16.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.16.8 Documentation Task (See Section 5.1.8 Core Expertise): Contractor shall produce written reports defining each inspection/evaluation to include, processes, procedures, findings, and recommendation. Due to the sensitivity of the reports they will only be reviewed by the NOSC Commander, appropriate section-head, or the individual themselves. Documents will be safeguarded in accordance with Privacy Act directives.

5.3.16.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall coordinate all evaluations with the appropriate section-head. Section-head will determine time and date of evaluations based on operational tempo and availability of personnel.

5.3.16.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.16.11 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.17 Web-Based Application Programmer/Developer (Deployable) Secret

- Contractor shall:
- Develop web pages and middleware applications using all versions of Hypertext Markup Language, C#, JavaScript, JQuery and other server and client-side languages.
- Optimize new and existing code for WAN performance.
- Integrate graphics, charts, and custom art into web sites to provide maximum impact of content delivery.
- Understand and apply AFI and DOD guidance on web development; ensures compliance, briefs management,
- Write and update concept of operations for web policy and implementation.
- Develop and manage training on materials, web pages, programming languages and third-party web applications used to support local and deployed internet and intranet web pages; includes classroom, and seminar training.
- Manage local and remote web servers; coordinate the mirroring of remote webs with a central mirrored site.

5.3.17.1 **Web Page Programming and Development Task:** Contractor shall develop globally accessible applications utilizing the latest web technologies focused on remote network management to provide help desk solutions for supporting deployed locations. Use .NET ASPX Pages, C#, Java, JavaScript, XML, XSLT, PowerShell, SharePoint, API compiled languages such as C++, and Open Database Control (ODBC) programming to access various ODBC sources and third-party software. Develop and ensure compliance to an approved

standard web motif. The motif will be applied to all subordinate web folders, pages, and web sites. Use manual and automated tools to ensure broken links are identified and corrected. Develop content to ensure web access is optimal for use on wide area network where bandwidth in low and latency is high. Content includes text, graphics, web art, menus, and index searching. Provide management with web site utilization reports. Report will provide status on access, utilization, and security.

5.3.17.2 **Training Support Task**: Contractor shall provide training support on web page development, content development, and maintenance. Develop procedures and best practice documents to be used by other web developers. Brief local and deployed web developers on standard practices, and AFI and DOD web development guidance to assist with web-based development of their products. Provide classroom training on an as required basis.

5.3.17.3 **OS Support Tasks**: Contractor shall understand the basics of the Microsoft and UNIX OS.

5.3.17.4 **Web Based Applications and Servers Task:** (See Section 5.1.5 Core Expertise): Contractor shall maintain Microsoft based web servers to include backups, disaster recovery, installation, troubleshooting, and data transfer. Contractor shall perform daily web server log review; comply with all security alerts to include loading patches and make registry changes to eliminate vulnerabilities. Web servers include the use of Microsoft SharePoint services (SPS) and SPS Portal servers.

5.3.17.5 **Network Security Task**: Contractor shall use security toolset to determine web server security weaknesses and shortfalls. Research and coordinate vulnerability finding with Security Analysis to provide fix actions. Apply security patches and validates compliance with security guidance.

5.3.17.6 **Documentation Task:** (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents for concept of operations (CONOPS), and tactics, techniques, and procedures (TTPs) on web-based development projects.

5.3.17.7 **Technical Coordinator Task**: (See Section 5.1.9 Core Expertise): Contractor shall provide technical support to other engineers when their project includes web-based or web-specific integration.

5.3.17.8 Technical Certifications Requirements: (See Section 5.1.10 Core Expertise)

5.3.18 Senior Web-Based Application Programmer/Developer (Deployable) Secret

- Contractor shall:
- Develop web pages and middleware applications using all versions of Hypertext Markup Language, and other server and client-side languages.
- Optimize new and existing code for WAN performance.

- Integrate graphics, charts, and custom art into web sites to provide maximum impact of content delivery.
- Understand and apply AFI and DOD guidance on web development; ensures compliance, briefs management,
- Write and update concept of operations for web policy and implementation.
- Develop and manage training on materials, web pages, programming languages and third-party web applications used to support local and deployed internet and intranet web pages; includes classroom, and seminar training.
- Manage local and remote web servers; coordinate the mirroring of remote webs with a central mirrored site.
- Manage work and project tasks of other web development contractors
- Mentor other NOSC engineers for professional development and career progression to include both technical and managerial growth.
- Review technical project documentation for final draft coordination and subsequent release. Includes assisting personnel with project documentation and web site development as needed.
- Coordinate technical visits from Air Force and other military agencies, and Contractors.

5.3.18.1 Web Page Programming and Development Task: Contractor shall develop globally accessible applications utilizing the latest web technologies focused on remote network management to provide help desk solutions for supporting deployed locations. Use .NET ASPX Pages, C#, Java, JavaScript, XML, XSLT, PowerShell, SharePoint API compiled languages such as C++, and Open Database Control (ODBC) programming to access various ODBC sources and third-party software. Develop and ensure compliance to an approved standard web motif. The motif will be applied to all subordinate web folders, pages, and web sites. Use manual and automated tools to ensure broken links are identified and corrected. Develop content to ensure web access is optimal for use on wide area network where bandwidth in low and latency is high. Content includes text, graphics, web art, menus, and index searching. Provide management with web site utilization reports. Report will provide status on access, utilization, and security. Training Support Task: Contractor shall provide training support on web page development, content development, and maintenance. Develop procedures and best practice documents to be used by other web developers. Brief local and deployed web developers on standard practices, and AFI and DOD web development guidance to assist with web-based development of their products. Provide classroom training on an as required basis.

5.3.18.2 OS Support Tasks: Contractor shall understand the basics of the Microsoft and UNIX OS.

5.3.18.3 Web Based Applications and Servers Task: (See Section 5.1.5 Core Expertise): Contractor shall maintain Microsoft based web servers to include backups, disaster recovery, installation, troubleshooting, and data transfer. Contractor shall perform daily web server log review; comply with all security alerts to include loading patches and make registry changes to eliminate vulnerabilities. Web servers include the use of Microsoft SharePoint services (SPS) and SPS Portal servers.

5.3.18.4 Network Security Task: Contractor shall use security toolset to determine web server security weaknesses and shortfalls. Research and coordinate vulnerability finding with Security Analysis to provide fix actions. Apply security patches and validates compliance with security guidance.

5.3.18.5 Documentation Task: (See Section 5.1.8 Core Expertise): Contractor shall develop and write technical documents for concept of operations (CONOPS), and tactics, techniques, and procedures (TTPs) on web-based development projects.

5.3.18.6 Technical Coordinator Task: (See Section 5.1.9 Core Expertise): Contractor shall provide technical support to other engineers when their project includes web-based or web-specific integration.

5.3.18.7 Technical Certifications Requirements: (See Section 5.1.10 Core Expertise)

5.3.18.8 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.19 Network Systems Web Architect Engineer (Deployable) Secret

- Contractor shall:
- Analyze a wide array of network, Web, and SharePoint metrics and recognize substandard network performance.
- Troubleshoot and develop solutions for network anomalies both remotely and locally.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Provide for crisis management during outages, virus outbreaks, and in high-pressure environments. Contractor shall possess a broad range of expertise in SharePoint architecture as deployed in a replicated enterprise environment.
- Use commercially available and local tools to analyze SharePoint and similar technology replication and provide recommendation to fix or enhance performance.

5.3.19.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.19.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.19.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.19.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.19.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.19.6 Network Security Tasks (See Section 5.1.6 Core Expertise): Contractor shall coordinate with the firewall administrators to ensure proper access control lists (ACL) and Internet Protocol (IP) filters are in place for network protection and security.

5.3.19.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.19.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.19.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise):

5.3.19.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.19.11 Replication Monitoring Task: Replication Monitoring Task: Contractor shall use Metalogix Replicator and Publisher to replicate and synchronize content, and look and feel of the USAFCENT Commander's Dashboard built on Microsoft SharePoint technology. The Contractor shall also proficient on the use and maintenance of Microsoft SQL Database replication.

5.3.20 Wireless Network Architecture Design Engineer (Deployable) Secret

- Contractor shall:
- Use extensive Wireless LAN background with designing WLAN architectures to provide proper coverage and support the ability for user to seamless move between WLAN access nodes without disconnection or other interruptions in service.
- Troubleshoot and develop solutions for wireless network anomalies both remotely and locally. Analyze a myriad of wireless networking metrics and recognize sub-par network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Determine if frequency interference issues are affecting the performance of the WLAN architecture.
- Troubleshoot network intrusion devices specific to the Department of Defense as well as many commercial information assurance tools to ensure proper design and integration;
- Posses strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco Switches and Routers, and hardware troubleshooting disciplines; who has a solid working knowledge of basic LAN technologies and OS used on deployed networks.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues. Must direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of skill sets tempered with confidence and leadership the Contractor shall be expected to function with minimal supervision.

5.3.20.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.20.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.20.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.20.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.20.5 Documentation Tasks (See Section 5.1.8 Core Expertise)

5.3.20.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.20.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.21 Systems/Network Engineer Subject Matter Expert (SME) (Deployable) Secret

- Contractor shall:
- Troubleshoot and develop solutions for network anomalies both remotely and locally.
- Analyze a myriad of networking metrics and recognize sub-standard network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Operate network protection and intrusion devices specific to the Department of Defense as well as many commercial information assurance tools.
- Demonstrate strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco, Microsoft, and hardware troubleshooting disciplines.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues.
- Direct, organize, and utilize crisis management processes and techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of technical skill sets tempered with confidence, leadership, and management capabilities to support the NOSC Operations Crew Commander.

5.3.21.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.21.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.21.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.21.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.21.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.21.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.21.7 Installation Tasks (See Section 5.1.7 Core Expertise): Uses knowledge gained from deployments and project installations to train and other active duty and contractor personnel on network and systems specific to AFCENT's network and systems environment.

5.3.21.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.21.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.21.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise): Contractor shall brief at the General Officer level on IT projects, upgrades, and specific issues.

5.3.22 Voice Protection Systems Engineer (Deployable) Secret

- Contractor shall:
- Troubleshoot and develop solutions for the Voice Protection System (VPS) anomalies both remotely and locally.
- Analyze and recognize sub-standard VPS performance and network interfacing modules.
- Develop reports and trend analysis documentation for the VPS
- Operate the VPS in accordance with Department of Defense and AFCENT policy
- Demonstrate strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel on VPS hardware and software troubleshooting disciplines
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent VPS problems/issues.
- Direct, organize, and utilize crisis management processes and techniques during operational outages and in high-pressure environments.
- Demonstrate expertise in a broad range of technical skill sets tempered with confidence, leadership, and management capabilities to support the NOSC Operations Crew Commander
- Provide recommendations on the daily operations of the VPS, and brief operational trending or isolated technical issues
- Maintain updated TTPs for VPS operation

- Develop draft VPS policy for AFCENT SPIN-C and periodically review and recommend changes

5.3.22.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.22.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.22.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.22.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.22.5 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.22.6 Installation Tasks (See Section 5.1.7 Core Expertise): Install and configure the VPS hardware and software following TTPs and standardized server configurations, hardware installation standards, and operational policies. Contractor will use knowledge gained from project installations to train active duty and contractor personnel on the VPS system specific to AFCENT's network and systems environment.

5.3.22.7 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.22.8 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.22.9 Technical Certifications Requirements (See Section 5.1.10 Core Expertise):

5.3.23 Senior Operational Support Team Manager (Deployable) TS/SCI

- Contractor shall:
- Possess and demonstrate a good understanding of geopolitical issues and interest related U.S. doctrine as applied to countries in the USAFCENT Area of Responsibility (AOR), Southwest Asia, especially in the areas of SharePoint, Network Health Assessment and Configuration Management.
- Stay current on technologies as applied to military and commercial Information Systems and Technologies to coordinate recommendations for both tactical and strategic planning purposes with USAFCENT/A6 and other senior staff on SharePoint, Network Health Assessment and Configuration Management subjects.
- Provide oral and written briefs and presentations to senior IT managers explaining and support recommendations on SharePoint, Network Health Assessment and Configuration Management subjects
- Maintain a professional image and appearance, including appropriate attire commensurate with this senior staff position. Profession business attire will be commensurate with government uniforms, and other contractor attire.
- Provide technical direction to other contractors on SharePoint, Network Health Assessment and Configuration Management concepts and apply System Development Life Cycle (SDLC) principles.

- Provide technical coordination and research to exploit cutting-edge technologies, assisting with technical and status updates for briefings and reporting on SharePoint, Network Health Assessment and Configuration Management subjects.
- Mentor other NOSC SharePoint, Network Health Assessment and Configuration Management engineers for professional development and career progression to include both technical and managerial growth.

- Establish and support the AFCENT Communications Control Board (CCCB) in accordance with Joint, CENTCOM, AF, and local Operating Instructions.
- Provide functional management of the CCCB, coordinate place and time of the CCCB with the board president and other voting members, collect and publish agenda items, record meeting minutes, and publish information on a secure web page.
- Monitor, processes, and manage the Systems Requirements Documents (AF3215) supporting the AFCENT mission.
- Review and coordinate all NOSC Communications Task Orders (CTO) submissions, and release to AFCENT Forward for publishing.
- Understand and apply AFI and DOD guidance on web development; write and update concept of operations for web policy and implementation.
- Manage the development of training materials, web pages, programming languages and third-party web applications used to support SharePoint on the AFCENT Enterprise to include classroom, and seminar training.
- Review technical project documentation for final draft coordination and subsequent release.
- Stay current on technologies as applied to military and commercial Information Systems and Technologies to coordinate recommendations for both tactical and strategic planning purposes with USAFCENT/A6 and other senior staff on IT subjects.
- Provide oral presentations and written briefs to senior military officers and IT managers.
- Provide technical coordination and research to exploit cutting-edge technologies, assisting with technical and status updates for briefings and reporting.
- Manage the development of technical documents based on extensive networking background in system administration or network engineering.
- Assists the Training Manager to develop/modify standardized training to meeting USAFCENT NOSC mission requirements and monitor local NOSC certifications and evaluations.
- Coordinate semi-annual site Staff Assistance Visits (SAV), or provides on-demand SAV at the request of deployed Senior Communications (SC); SAV augmentation may come from other DoD resources or internal NOSC resources.
- Review standard systems and network processes and checklist to validate they meet prescribed standards, and are easily executed from a comprehensive checklist.
- Coordinate technical visits from DoD personnel and commercial vendors
- Review SharePoint, Network Health Assessment and Configuration Management technical project documentation for final draft coordination and subsequent release. Includes assisting personnel with project documentation and web site development as needed.

5.3.23.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.23.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.23.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.23.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.23.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.23.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.23.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.23.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.23.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise): Contractor shall research cutting edge SharePoint, Network Health Assessment and Configuration Management technologies to determine applicability to the USAFCENT data-networking mission. Contractor shall be primary point of contact with technology vendors for using commercial-off-the-shelve (COTS) technology, and custom designed and engineered solutions specific to the USAFCENT. However, the Contractor shall not negotiate with vendors on changes or new requirements that could obligate the government, or incur charges.

5.3.23.10 Briefing and Presentation Task: Contractor shall use Microsoft Power Point to prepare briefings and presentations in support of SharePoint, Network Health Assessment and Configuration Management initiatives. Briefing will be delivered to the USAFCENT/A6 and other senior staff on an as required basis, and will typically include pre and post symposium and conference briefing. Briefing will be provided in both oral and written formats. Contractor shall assist the Chief of Operating Support Team (OST) to provide technical and status updates to the NOSC commander on a weekly basis. Contractor must be prepared to brief all OST project and production issues with little or no-notice.

5.3.23.11 Mentoring and Profession Development Task: Contractor shall support military and contractor data and systems engineers offering technical and management experience with project management and development. This includes assisting with the writing of Concept of Operations, Engineering Plans, Special Instructions for Communicators (SINC), and other technical documentation. Assists OST Leads with determining project scope, timelines, list of materials, coordination meetings, and general project management as required.

5.3.23.12 Technical Project Review Task: Contractor shall review final draft of all technical OST documentation for both data and systems projects. “Final-Draft” documents will be submitted for inclusion with other project documentation for final coordination.

5.3.23.13 Coordination and Liaison Task: Contractor shall coordinate visits from Air Force, other military agencies, and Contractors. Contractor shall coordinate the schedule to prevent conflicts with other OST projects and schedules and to maximize effectiveness of visits and use of resources. Contractor shall coordinate the need to allocate NOSC resources with senior staff.

5.3.23.14 Trip Reporting Documentation Task: All trip reports will be full documented and are due within five duty days of return. Trip reports will be provided for all Conferences, Seminars, In-Progress Reviews, Technical Development and Engineering Studies. Trip reports will be in standard AF format and delivered to the Chief of Operations Support Team for review.

5.3.23.15 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.23.16 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

5.3.24 Wide Area Network Architecture & Design Engineer (Deployable) Secret

Contractor shall:

- Use extensive LAN/WAN background with designing External Gateway Protocol (EGP) such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), and Interior Gateway Protocol (IGP) such as and Enhanced Interior Gateway Routing Protocol (EIGRP).
- Troubleshoot and develop solutions for network anomalies both remotely and locally. Analyze a myriad of networking metrics and recognize sub-par network performance.
- Configure, monitor and trouble-shoot National IP/MPLS backbone network.
- Good understanding of Quality of Service (QOS) and Hands on experience of QOS on Cisco
- Configuring and troubleshooting QOS involving policing, shaping, shaping and queuing from CE towards PE routers
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Possess strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco Switches and Routers, and hardware troubleshooting disciplines; who has a solid working knowledge of basic LAN technologies and OS used on deployed networks.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues. Must direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of skill sets tempered with confidence and leadership the Contractor shall be expected to function with minimal supervision.

Perform analysis for collaboration of network / system needs and participate in planning, designing, upgrading and deployment of enterprise datacenter hardware and software using a project based timeline.

5.3.24.1 General Networking Tasks (See Section 5.1.1 Core Expertise)
5.3.24.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)
5.3.24.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)
5.3.24.4 OS Support Tasks (See Section 5.1.4 Core Expertise)
5.3.24.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)
5.3.24.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.24.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.24.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.24.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.24.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.3.25 Unified Collaboration Architecture & Design Engineer (Deployable) Secret

Contractor shall:

- Exhibit knowledge on Cisco Unified Commination Call Manager, Unity, Unity Connection & Unity Express
- Demonstrate strong understanding of Cisco Unified Communication Dial Plans, Calling Search Spaces and Partitions
- Have experience with VOIP Products and platforms
- Troubleshoot escalated issues to identify and repair complex network issues for WAN, LAN, Voice or Video connections.
- Comprise Implementation knowledge of QoS and CAC, troubleshooting complex network regarding call routing and gateways
- Possess Strong understanding of VoIP QoS issues and mitigation strategies
- Troubleshoot and develop solutions for network anomalies both remotely and locally. Analyze a myriad of networking metrics and recognize sub-par network performance.
- Develop reports and trend analysis documentation on bandwidth and network security incidents.
- Possess strong interpersonal skills and sufficient mastery of the IT profession to act as an on-shift training representative for both contractors and government personnel to include Cisco Switches and Routers, and hardware troubleshooting disciplines; who has a solid working knowledge of basic LAN technologies and OS used on deployed networks.
- Utilize data at hand to make expert decisions and recommendations on how to resolve, improve, or prevent network problems/issues. Must direct, organize, and utilize crisis management techniques during outages, virus outbreaks, and in high-pressure environments.
- Demonstrate expertise in a broad range of skill sets tempered with confidence and leadership the Contractor shall be expected to function with minimal supervision.
- Use advanced technical writing skills to develop and update IT systems concept of operations and engineering plans.

5.3.25.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.25.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.25.3 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.25.4 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.25.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.3.25.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.25.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide

requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications.

5.3.25.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.25.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

Technical Certifications Requirements (See Section 5.1.10 Core Expertise

5.3.26 Senior Technical Advisor/Architect (Deployable) TS/SCI

Contractor shall:

- Assist the USAFCENT A6O Technical Director with developing the strategic direction, goals, objectives and implementation strategy for IT services provided throughout the countries in the USAFCENT Area of Responsibility (AOR), Southwest Asia.
- Provide strategic guidance and technical direction across all USAFCENT A6O functional areas on network and systems engineering to develop network and systems engineering concepts and apply System Development Life Cycle (SDLC) principles
- Balances workload and provides direction and guidance regarding organization policies, procedures and guidelines.
- Plans, directs and executes all USAFCENT network operations projects supporting USCENTCOM contingency and wartime operations
- Possess and demonstrate a good understanding of geopolitical issues and interest related U.S. doctrine as applied to countries in the USAFCENT Area of Responsibility (AOR), Southwest Asia, especially in the areas of IT.
- Stay current on technologies as applied to military and commercial Information Systems and Technologies to coordinate recommendations for both tactical and strategic planning purposes with USAFCENT/A6 and other senior staff on IT subjects.
- Evaluates new and emerging IT technologies and security methods to ensure successful integration with existing and anticipated infrastructure environment
- Participate in planning conferences and working groups to represent the IT strategy and objectives of USAFCENT.
- Provide oral and written briefs and presentations to senior IT managers explaining and support recommendations.
- Maintain a professional image and appearance, including appropriate attire commensurate with this senior staff position. Profession business attire will be commensurate with government uniforms, and other contractor attire.
- Provide technical coordination and research to exploit cutting-edge technologies, assisting with technical and status updates for briefings and reporting.
- Mentor other NOSC engineers for professional development and career progression to include both technical and managerial growth.
- Review technical project documentation for final draft coordination and subsequent release. Includes assisting personnel with project documentation and web site development as needed.
- Coordinate technical visits from Air Force, other military agencies and contractors.
- Meet with key vendors and other organizations to represent USAFCENT A6 requirements.

5.3.33.1 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.3.33.2 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.3.33.3WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.3.33.4OS Support Tasks (See Section 5.1.4 Core Expertise)

5.3.33.5 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)5.3.33.6 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.3.33.7 Installation Tasks (See Section 5.1.7 Core Expertise): Contractor is required to deploy as a member of a project installation team. This worldwide requirement will necessitate a valid US Passport. Contractor must be available to deploy worldwide without medical/personal complications. Contractor must be prepared (with appropriate attire) to make a formal presentation to Senior Host Nation IT staff on project details with little notice.

5.3.33.8 Documentation Task (See Section 5.1.8 Core Expertise)

5.3.33.9 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.3.33.10 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.4 USAFCENT Off-Site Tasks

5.4.1 Network Defense and Security Analyst (Non-Deployable) TS/SCI

- Contractor shall:
- Work with other contractors' Team Leaders and the Government Contracting Officer's Representative (COR) to accomplish Government requirements, goals, and mission objectives as efficiently and effectively as possible. This shall include, but is not limited to, sharing or coordinating information resulting from the work required by this SOW or previous Government efforts and working as a team to perform tasks in concert.
- Assist other active duty, government civilians, and contractors assigned to the same functional areas to raise the level of proficiency and effectiveness of the team performing that function.
- Provide technical reports, meeting minutes, program plans, concepts of operations, contingency plans, and related documentation as identified for task deliverables
- Prepare and disseminate operational reports. A list of operational reports shall include, but is not limited to, AF Computer Emergency Response Team (AFCERT) daily operations report (DOR), operation report (OPREP), and situational report (SITREP), incident response, law enforcement, and recovery operations reports, Information protection bulletins (IP Bulletins), AFCERT Time Compliance Network Orders (TCNOs), malicious logic/virus notifications, INFOCONs, and other messages.
- Support real-time monitoring of all assigned IPS/IPS deployed and supporting the AFCENT/CENTCOM mission
- Monitor network traffic to provide event correlations of operational traffic from multiple locations to determine network security posture
- Use standard/provided network tools to evaluate traffic for incident response analysis
- Coordinate and execute JTF-GNO Information Assurance Vulnerability Alert (IAVA) notices as applicable on CENTCOM networks/systems with the AFCENT NOSC
- Maintain IDS/IPS devices to ensure they are operating at optimal efficiency
- Maintain Crew certification as required to operate on CENTCOM, AFCENT, and AF networks

5.4.1.1 **IDS/IPS Real-Time Monitoring Analysis Task:** The contractor shall:

- Conduct network security monitoring and intrusion detection analysis using the AFCENT/CENTCOM security tools to include but is not limited to IDS/IPS, firewall, proxy, router logs. Mission-specific operational training (i.e., process/procedures and checklist familiarization) will be conducted by the government to maintain operational proficiency. The contractor shall be trained, tested, certified, and periodically evaluated by Stan/Eval processes IAW operational position requirements.
- Research Net Defense (NetD) events to determine the necessity for deeper analysis and conduct an initial assessment of type and extent of intruder activities. Enters event data into mission support systems according to operational procedures and reports to meet AFCENT mission/tasking. The contractor shall produce a Suspicious Event Report (SER) for suspicious traffic meeting established thresholds. These SERs shall contain sufficient information to facilitate future research of suspicious traffic. The SERs shall answer the who, why and when for this suspicious activity. The contractor shall compile SERs and other artifacts to support event escalation to Incident Response.
- Provide pass-on information to bring incoming crews up to speed on latest suspicious traffic seen from a given port, IP, etc. The contractor shall coordinate with the Crew Commander for authorization before departing after pass-on to incoming shift.
- Provide reporting and computer security-related assistance to AFCENT Network Operations & Security Center in countering vulnerabilities, minimizing risk, and improving the security posture of CENTCOM computer networks and systems supporting AFCENT's operational requirements and mission execution.
- Provide focused NetD, tailored analysis and monitoring operations of specified sensor locations during contingency operations and in support of named NetD operations and exercises.
- Track trends of authorized an unauthorized activity
- Correlate unusual and suspicious network activity across CENTCOM. Validate unusual network activity unique to a geographical regions and sensor locations
- Provide an overall site-analysis profile to serve as a benchmark to identify unusual or suspicious activity
- Assist in completion of NetD statistical and trend data and operational event reporting when requested
- Maintain current knowledge on new vulnerabilities and exploits. Develop methods to detect and prevent intrusive activities utilizing these new vulnerabilities and exploits. Assist NOSC-IA to develop countermeasures (to include IDS/IPS signature development and correlation rule sets) to isolate, contain and prevent intrusive actives and secure AFCENT/CENTCOM networks

5.4.1.2 **Network Event Correlation/Advanced Traffic Analysis Task:** The contractor shall:

- Possess the following skill sets: experience with DoD/AF incident reporting processes; familiarity with NSA Threat Operations Center (NTOC) Attack, Sensing & Warning (AS&W) alerts and processing; knowledge and experience constructing, executing and troubleshooting SQL DB queries; knowledge and experience with the DoD Centaur analysis system. The contractor shall maintain their respective Advanced Traffic Analyst certification via Stan/Eval processes for operational positions.

- Provide site-specific and service-level intrusion packet level analysis using selected tools and activities related to mission execution. Track trends of authorized and unauthorized activity.
- Correlate unusual and suspicious network activity across CENTCOM. Validate unusual network activity unique to geographical regions and sensor location(s).
- Document network devices and location of network devices. Provide technical information to CENTCOM customers on devices with an emphasis on any possible security issues with them. Document any waivers from standard network configurations.
- Provide an overall site-analysis and profile for existing CENTCOM networks and supported units to serve as a benchmark to identify unusual or suspicious activity. Research, document and report suspicious activity IAW established procedures.
- Provide focused NetD, tailored analysis and monitoring operations of specified sensor locations during contingency operations and in support of named NetD operations and exercises.
- Assist in the compilation of NetD statistical and trend data and operational event reporting when requested by AFCENT NOSC management.

5.4.1.3 **Incident Response Analysis Task:** The contractor shall:

- Possess the following skill sets: extensive knowledge of network firewalls, computer and server log analysis, computer network servers (DNS, proxy, e-mail, domain controller, file server, Active Directory) and analysis of their logs; extensive knowledge of digital evidence collection, handling and security; experience with computer incident response and analysis and report dissemination; extensive knowledge and experience with network packet capture and analysis software such as WireShark (Ethereal) and Snort; experience with standard DoD network topology and DMZ boundary protection; experience with system analysis software (i.e. EnCase/EnCase Enterprise or FTK), software coding and debugging, and the virtual machine (VM) environment.
- Perform network traffic analysis to evaluate intruder activities using host and network-based monitoring systems. Correlate information gathered to provide CENTCOM networks effective methods to protect their domains. Determine the probability of exploitation of discovered network vulnerabilities. Ensure appropriate notification action is taken to reduce the risk to all CENTCOM networks.
- Support CENTCOM 24/7 NetD monitoring operations. Upon identification of suspicious activity on CENTCOM networks, open and conduct network intrusion investigations to validate the unauthorized activity and determine the type and extent of activity.
- Conduct network and computer forensics on suspected and confirmed compromised CENTCOM systems to determine the method of intrusion and corrective actions to be taken to prevent or detect similar future activities.

- Develop methods to identify, contain, log, and analyze intrusive activities and security vulnerabilities on Air Force Automated Information Systems (AIS) and networks. Prevent intruders from accessing Air Force resources. Maintain current knowledge on new vulnerabilities and exploits. Develop methods to detect and prevent intrusive activities utilizing these new vulnerabilities and exploits. Conduct operations and develop countermeasures (to include IDS/IPS signature development and correlation rule

sets) to isolate, contain, and prevent intrusive activities and security vulnerabilities on Air Force AIS and networks.

- Maintain current knowledge on existing and new malware behavior and propagation characteristics. Maintain current knowledge on the anti-virus tools currently in use in CENTCOM. Develop methods to identify, contain, log, and analyze malware-based activities on Air Force AIS and networks. Provide specialized anti-virus assistance and support to CENTCOM field units.
- Provide AFOSI (Air Force Office of Special Investigation), Army Criminal Investigation Division (CID), Naval Criminal Investigation Service (NCIS) NetD technical support and expertise to assist law enforcement and counter-intelligence activities. Continue to conduct base network defense while Component investigation agencies collects network evidence. Provide support to CENTCOM network administrators on the installation and analysis of packet sniffers on their network topology.

5.4.1.4 **Vulnerability Analysis Task:** The contractor shall:

- Possess the following skill sets: experience with DoD/AF incident reporting processes; knowledge of threat visualization applications; extensive knowledge of digital evidence collection, handling and security; experience with computer incident response and analysis, and report dissemination; extensive knowledge of DoD and AF network operations regulations; knowledge and experience processing Information Assurance Vulnerability Alert (IAVA) notices.
- Provide technical standardization of time critical reports, manage historical documentation, and maintain on-line vulnerability tracking and incident response databases. Support development of AF Cyber Incident Reports (AFCIR) and coordinate staffing and approval of security reviews of all AFCIRs.

5.4.1.5 **IDS/IPS Sensor Maintenance Task:** The contractor shall:

- Install, configure, maintain and manage the AFCENT IDS/IPS sensor fleet, ArcSight Enterprise Security Manager, CIDDS directors, and associated Virtual Private Network (VPN) equipment/configurations. Assist in the development and documentation of sensor processes and checklists.
- Maintain and manage the capability to upgrade software and perform system changes for the IDS/IPS sensor fleet and associated VPN equipment. Maintain and manage the capability to deploy additional new string matches and alerts to all deployed IDS/IPS sensors in support of CENTCOM operations, to include developing, testing and maintaining custom IDS/IPS signatures.
- Support CENTCOM operations by providing the capability to "omit" or filter sensor traffic and alerts reporting activity based on AFCENT NOSC-IA's instruction that traffic does not need to be reviewed in a "real-time" operation by analysts.

- Monitor the effectiveness of the IDS/IPS sensor's ability to collect and report suspicious network activity on CENTCOM Theater Information Grid (TIG). Perform immediate diagnostic testing and troubleshooting either remotely or coordinate actions of a local network system administrator having direct access to the IDS/IPS sensor through AFCENT NOSC-IA.

- Conduct troubleshooting and fault isolation to ensure network connectivity between the directors and sensor equipment. Establish VPNs between AF and CENTCOM sites for protected communications. Maintain commercial off the shelf (COTS) and access control lists to restrict unauthorized access to network. Create and manage user accounts. Assign the users specific rights to access network resources.
- Provide technical advice and assistance to the AFCENT NOSC-IA to resolve network issues and perform actions necessary to ensure IDS/IPS sensors are collecting and reporting network activity. Diagnose and resolve end user problems. Ensure the end users adhere to the proper security policies and procedures.

5.4.1.6 **IDS/IPS Database & VPN Technical Support Task:** The contractor shall:

- Provide technical support to IDS/IPS, CIDDS, ArcSight, GRIDD and related VPN and CDS system administration and operations. Assist in the conduct of the daily private key management.
- Support IDS/IPS software installation and configuration, IDS site troubleshooting, system security, archival, and restoration of mission data.
- Ensure that response to inoperable systems (e.g., IDS/IPS, CIDDS ArcSight, GRIDD and CDS related VPN) or encrypted communications is within one hour.
- Assist in the identification of system and network configuration problems or network and subnet vulnerabilities and take corrective actions.

5.4.1.7 Network Defense Training and Instruction Task: The contractor shall:

- Ensure all Initial Qualification Training instructors are designated crew certified analysts. In order to maintain this certification and proficiency, instructors shall be required to work crew positions as defined in local operating instructions.
- Provide training and support personnel to further enhance their organizational, analytical and functional knowledge of computer security, system vulnerabilities, exploits, related digital signatures, hacking patterns, and countermeasures.
- Develop and document training objectives, in coordination with Government COR, for review and approval. The contractor shall assist in developing, documenting, and maintaining appropriate training plans.
- Assist with on-the-job training (OJT) of individuals assigned to AFCENT operational mission and technical support.
- Present AFCENT and CENTCOM mission briefing for applicability of NetD actions to warfighting customer

5.4.1.8 Standardization & Evaluation (Stan/Eval) Task: The contractor shall:

- Provide technical guidance and assistance to the government in developing, implementing and maintaining an operational Stan/Eval and crew assessment program, to include scheduling and conducting assessments.
- Assist in the creation of monthly technical reports of squadron Stan/Eval results.

5.4.1.9 Operational Process Tracking and Processing Task: The contractor shall:

- Comply with the applicable requirements outlined in paragraph 3.11 and 3.12.
- Serve as a central point of contact for receiving information pertaining to the integration of processes, Stan/Eval, and NetD (TTPs).

- Identify and assist in the development and documentation of AFCENT support operations, reporting, systems administration and incident response processes and tasks using available mission support systems.
- Spearhead process coordination within the Squadron and externally.
- Maintain library of approved processes and distributes.
- Document the proceedings of the Operational Process Panel to track status of updates or new TTPs. The Operational Process Panel shall convene on a monthly basis or as determined by the DO or his designated appointee. The purpose of this panel is to review and accept or reject updates to processes and checklists.

5.4.1.10 Systems Planning Task: The contractor shall:

- Provide technical assistance in the planning, testing, development, implementation, enhancement, transition, management and operations of new AFCENT initiatives. Support the integration of these systems into existing architecture.
- Maintain a current status of program plan milestones and historical records for new initiatives.
- Assist in NetD exercise support planning.
- Attend technical interchange meetings (TIMs) to assist in the planning, testing, development, and transition towards the implementation of newer and more advanced versions of AFCENT tools and architecture. Provide the technical trip report to the QAP and AFCENT NOSC-IA within five (5) duty days of travel IAW local directives.

5.4.1.11 **Technical Interchange Meeting Task**: Conduct a technical interchange meeting (TIM) within sixty (60) work days of contract award and quarterly thereafter, within 3 business days of notification. The TIM shall be held at the government facility. For all TIMs the contractor shall provide an agenda for the meeting and minutes after the meeting. The minutes are due to the COR and AFCENT NOSC-IA within fifteen (15) working days after the TIM. Deliverables provided on this contract shall be provided in hardcopy (paper) and software versions (Microsoft Word/PowerPoint/Excel) compatible format. Deliverables shall be delivered/uploaded to ITSS.

5.4.1.12 **Network Defense Technical Report Task:** Deliver a technical report of the results of NetD operations, including IDS/IPS analysis, requirement reports, tool deficiency reports, lessons-learned reports, in accordance with established procedures within assigned suspense. A report shall be generated at the completion of each Task. The contractor shall provide oral and written technical communications to NetD managers including, but not limited to, procedural documentation, operations reports, plans of action, incident logs, and related material. Technical reports shall be provided in Microsoft Word/PowerPoint/Excel compatible format. Suspense date extensions shall be requested at least two (2) duty days in advance.

5.4.1.13 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.4.1.14 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.4.1.15 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.4.1.16 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.4.1.17 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.4.1.18 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.4.1.19 Documentation Task (See Section 5.1.8 Core Expertise)

5.4.1.20 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.4.1.21 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.4.1.22 Educational Requirements (See Section 5.1.10 Core Expertise)

5.4.2 Senior Network Defense and Security Analyst (Task Lead) (Non-Deployable) TS/SCI

Contractor shall:

- Ensure that the Monthly Status Report is provided IAW PWS directions.
- Work with other contractors' Team Leaders and the Government Contracting Officer's Representative (COR) to accomplish Government requirements, goals, and mission objectives as efficiently and effectively as possible. This shall include, but is not limited to, sharing or coordinating information resulting from the work required by this SOW or previous Government efforts and working as a team to perform tasks in concert.
- Assist other active duty, government civilians, and contractors assigned to the same functional areas to raise the level of proficiency and effectiveness of the team performing that function.
- Provide technical reports, meeting minutes, program plans, concepts of operations, contingency plans, and related documentation as identified for task deliverables
- Prepare and disseminate operational reports. A list of operational reports shall include, but is not limited to, AF Computer Emergency Response Team (AFCERT) daily operations report (DOR), operation report (OPREP), and situational report (SITREP), incident response, law enforcement, and recovery operations reports, Information protection bulletins (IP Bulletins), AFCERT Time Compliance Network Orders (TCNOs), malicious logic/virus notifications, INFOCONs, and other messages.
- Support real-time monitoring of all assigned IPS/IPS deployed and supporting the AFCENT/CENTCOM mission
- Monitor network traffic to provide event correlations of operational traffic from multiple locations to determine network security posture
- Use standard/provided network tools to evaluate traffic for incident response analysis
- Coordinate and execute JTF-GNO Information Assurance Vulnerability Alert (IAVA) notices as applicable on CENTCOM networks/systems with the AFCENT NOSC
- Maintain IDS/IPS devices to ensure they are operating at optimal efficiency

- Maintain Crew certification as required to operate on CENTCOM, AFCENT, and AF networks

5.4.2.1 **IDS/IPS Real-Time Monitoring Analysis Task:** The contractor shall:

- Track trends of authorized an unauthorized activity
- Correlate unusual and suspicious network activity across CENTCOM. Validate unusual network activity unique to a geographical regions and sensor locations
- Provide an overall site-analysis profile to serve as a benchmark to identify unusual or suspicious activity
- Assist in completion of NetD statistical and trend data and operational event reporting when requested
- Maintain current knowledge on new vulnerabilities and exploits. Develop methods to detect and prevent intrusive activities utilizing these new vulnerabilities and exploits. Assist NOSC-IA to develop countermeasures (to include IDS/IPS signature development and correlation rule sets) to isolate, contain and prevent intrusive actives and secure AFCENT/CENTCOM networks

5.4.2.2 **Network Event Correlation/Advanced Traffic Analysis Task:** The contractor shall:

- Possess the following skill sets: experience with DoD/AF incident reporting processes; familiarity with NSA Threat Operations Center (NTOC) Attack, Sensing & Warning (AS&W) alerts and processing; knowledge and experience constructing, executing and troubleshooting SQL DB queries; knowledge and experience with the DoD Centaur analysis system. The contractor shall maintain their respective Advanced Traffic Analyst certification via Stan/Eval processes for operational positions.
- Provide site-specific and service-level intrusion packet level analysis using selected tools and activities related to mission execution. Track trends of authorized and unauthorized activity.
- Correlate unusual and suspicious network activity across CENTCOM. Validate unusual network activity unique to geographical regions and sensor location(s).
- Document network devices and location of network devices. Provide technical information to CENTCOM customers on devices with an emphasis on any possible security issues with them. Document any waivers from standard network configurations.
- Provide an overall site-analysis and profile for existing CENTCOM networks and supported units to serve as a benchmark to identify unusual or suspicious activity. Research, document and report suspicious activity IAW established procedures.
- Provide focused NetD, tailored analysis and monitoring operations of specified sensor locations during contingency operations and in support of named NetD operations and exercises.
- Assist in the compilation of NetD statistical and trend data and operational event reporting when requested by AFCENT NOSC management.

5.4.2.3 **Incident Response Analysis Task:** The contractor shall:

- Possess the following skill sets: extensive knowledge of network firewalls, computer and server log analysis, computer network servers (DNS, proxy, e-mail, domain controller, file server, Active Directory) and analysis of their logs; extensive knowledge of digital

evidence collection, handling and security; experience with computer incident response and analysis and report dissemination; extensive knowledge and experience with network packet capture and analysis software such as WireShark (Ethereal) and Snort; experience with standard DoD network topology and DMZ boundary protection; experience with system analysis software (i.e. EnCase/EnCase Enterprise or FTK), software coding and debugging, and the virtual machine (VM) environment.

- Perform network traffic analysis to evaluate intruder activities using host and network-based monitoring systems. Correlate information gathered to provide CENTCOM networks effective methods to protect their domains. Determine the probability of exploitation of discovered network vulnerabilities. Ensure appropriate notification action is taken to reduce the risk to all CENTCOM networks.
- Support CENTCOM 24/7 NetD monitoring operations. Upon identification of suspicious activity on CENTCOM networks, open and conduct network intrusion investigations to validate the unauthorized activity and determine the type and extent of activity.
- Conduct network and computer forensics on suspected and confirmed compromised CENTCOM systems to determine the method of intrusion and corrective actions to be taken to prevent or detect similar future activities.
- Develop methods to identify, contain, log, and analyze intrusive activities and security vulnerabilities on Air Force Automated Information Systems (AIS) and networks. Prevent intruders from accessing Air Force resources. Maintain current knowledge on new vulnerabilities and exploits. Develop methods to detect and prevent intrusive activities utilizing these new vulnerabilities and exploits. Conduct operations and develop countermeasures (to include IDS/IPS signature development and correlation rule sets) to isolate, contain, and prevent intrusive activities and security vulnerabilities on Air Force AIS and networks.
- Maintain current knowledge on existing and new malware behavior and propagation characteristics. Maintain current knowledge on the anti-virus tools currently in use in CENTCOM. Develop methods to identify, contain, log, and analyze malware-based activities on Air Force AIS and networks. Provide specialized anti-virus assistance and support to CENTCOM field units.
- Provide AFOSI (Air Force Office of Special Investigation), Army Criminal Investigation Division (CID), Naval Criminal Investigation Service (NCIS) NetD technical support and expertise to assist law enforcement and counter-intelligence activities. Continue to conduct base network defense while Component investigation agencies collects network evidence. Provide support to CENTCOM network administrators on the installation and analysis of packet sniffers on their network topology.

5.4.2.4 **Vulnerability Analysis Task:** The contractor shall:

- Possess the following skill sets: experience with DoD/AF incident reporting processes; knowledge of threat visualization applications; extensive knowledge of digital evidence collection, handling and security; experience with computer incident response and analysis, and report dissemination; extensive knowledge of DoD and AF network operations regulations; knowledge and experience processing Information Assurance Vulnerability Alert (IAVA) notices.
- Provide technical standardization of time critical reports, manage historical documentation, and maintain on-line vulnerability tracking and incident response databases. Support development of AF Cyber Incident Reports (AFCIR) and coordinate staffing and approval of security reviews of all AFCIRs.

5.4.2.5 **IDS/IPS Sensor Maintenance Task:** The contractor shall:

- Install, configure, maintain and manage the AFCENT IDS/IPS sensor fleet, ArcSight Enterprise Security Manager, CIDDS directors, and associated Virtual Private Network (VPN) equipment/configurations. Assist in the development and documentation of sensor processes and checklists.
- Support CENTCOM operations by providing the capability to "omit" or filter sensor traffic and alerts reporting activity based on AFCENT NOSC-IA's instruction that traffic does not need to be reviewed in a "real-time" operation by analysts.
- Provide technical advice and assistance to the AFCENT NOSC-IA to resolve network issues and perform actions necessary to ensure IDS/IPS sensors are collecting and reporting network activity. Diagnose and resolve end user problems. Ensure the end users adhere to the proper security policies and procedures.

5.4.2.6 **IDS/IPS Database & VPN Technical Support Task:** The contractor shall:

- Provide technical support to IDS/IPS, CIDDS, ArcSight, GRIDD and related VPN and CDS system administration and operations. Assist in the conduct of the daily private key management.
- Support IDS/IPS software installation and configuration, IDS site troubleshooting, system security, archival, and restoration of mission data.
- Ensure that response to inoperable systems (e.g., IDS/IPS, CIDDS ArcSight, GRIDD and CDS related VPN) or encrypted communications is immediate.
- Assist in the identification of system and network configuration problems or network and subnet vulnerabilities and take corrective actions.

5.4.2.7 Network Defense Training and Instruction Task: The contractor shall:

- Ensure all Initial Qualification Training instructors are designated crew certified analysts. In order to maintain this certification and proficiency, instructors shall be required to work crew positions as defined in local operating instructions.
- Provide training and support personnel to further enhance their organizational, analytical and functional knowledge of computer security, system vulnerabilities, exploits, related digital signatures, hacking patterns, and countermeasures.
- Develop and document training objectives, in coordination with Government COR, for review and approval. The contractor shall assist in developing, documenting, and maintaining appropriate training plans.
- Assist with on-the-job training (OJT) of individuals assigned to AFCENT operational mission and technical support.
- Present AFCENT and CENTCOM mission briefing for applicability of NetD actions to warfighting customer

5.4.2.8 Standardization & Evaluation (Stan/Eval) Task: The contractor shall:

- Provide technical guidance and assistance to the government in developing, implementing and maintaining an operational Stan/Eval and crew assessment program, to include scheduling and conducting assessments.

- Assist in the creation of monthly technical reports of squadron Stan/Eval results.

5.4.2.9 Operational Process Tracking and Processing Task: The contractor shall:

- Comply with the applicable requirements outlined in paragraph 3.11 and 3.12.
- Serve as a central point of contact for receiving information pertaining to the integration of processes, Stan/Eval, and NetD (TTPs).
- Identify and assist in the development and documentation of AFCENT support operations, reporting, systems administration and incident response processes and tasks using available mission support systems.
- Spearhead process coordination within the Squadron and externally.
- Maintain library of approved processes and distributes.
- Document the proceedings of the Operational Process Panel to track status of updates or new TTPs. The Operational Process Panel shall convene on a monthly basis or as determined by the DO or his designated appointee. The purpose of this panel is to review and accept or reject updates to processes and checklists.

5.4.2.10 Systems Planning Task: The contractor shall:

- Provide technical assistance in the planning, testing, development, implementation, enhancement, transition, management and operations of new AFCENT initiatives. Support the integration of these systems into existing architecture.
- Maintain a current status of program plan milestones and historical records for new initiatives.
- Assist in NetD exercise support planning.
- Attend technical interchange meetings (TIMs) to assist in the planning, testing, development, and transition towards the implementation of newer and more advanced versions of AFCENT tools and architecture. Provide the technical trip report to the QAP and AFCENT NOSC-IA within five (5) duty days of travel IAW local directives.

5.4.2.11 **Technical Interchange Meeting Task**: Conduct a technical interchange meeting (TIM) within sixty (60) work days of contract award and quarterly thereafter, within 3 business days of notification. The TIM shall be held at the government facility. For all TIMs the contractor shall provide an agenda for the meeting and minutes after the meeting. The minutes are due to the COR and AFCENT NOSC-IA within fifteen (15) working days after the TIM. Deliverables provided on this contract shall be provided in hardcopy (paper) and software versions (Microsoft Word/PowerPoint/Excel) compatible format.

5.4.2.12 **Network Defense Technical Report Task:** Deliver a technical report of the results of NetD operations, including IDS/IPS analysis, requirement reports, tool deficiency reports, lessons-learned reports, in accordance with established procedures within assigned suspense. A report shall be generated at the completion of each sub-task. The contractor shall provide

oral and written technical communications to NetD managers including, but not limited to, procedural documentation, operations reports, plans of action, incident logs, and related material. Technical reports shall be provided in Microsoft Word/PowerPoint/Excel compatible format. Suspense date extensions shall be requested at least two (2) duty days in advance.

5.4.2.13 General Networking Tasks (See Section 5.1.1 Core Expertise)

5.4.2.14 LAN Support Tasks (See Section 5.1.2 Core Expertise)

5.4.2.15 WAN/Enterprise Support Tasks (See Section 5.1.3 Core Expertise)

5.4.2.16 OS Support Tasks (See Section 5.1.4 Core Expertise)

5.4.2.17 Web Based Applications and Servers Tasks (See Section 5.1.5 Core Expertise)

5.4.2.18 Network Security Tasks (See Section 5.1.6 Core Expertise)

5.4.2.19 Documentation Task (See Section 5.1.8 Core Expertise)

5.4.2.20 Technical Coordinator Task (See Section 5.1.9 Core Expertise)

5.4.2.21 Technical Certifications Requirements (See Section 5.1.10 Core Expertise)

5.4.2.22 Educational Requirements (See Section 5.1.10 Core Expertise): This position requires a formal education commensurate with the level of military contemporaries. Briefs at the general officer level on IT projects, upgrades, and specific issues.

6.0 Meetings/Reports.

6.1.1 Kick-off meeting. A preparatory, kick-off meeting shall be held no later than seven (7) working days after award of this delivery order. The government representatives and contractor shall meet at a location determined by the government/client representative(s).

6.1.2 Progress reports**.** Monthly progress reports shall be prepared by the contractor and delivered to the government/client representative via ITSS.

6.1.3 Technical Reports. The Contractor shall produce a monthly technical progress report in standard contractor format, and provide a compiled monthly report for all sites and exercises supported. The monthly report will include reports for completed trips associated with this task and the following items on an as needed basis.

a. Conduct periodic technical evaluations of the USAFCENT LAN to verify proper interoperability and integration with current/future operating systems and networks.

b. Identify equipment and software deficiencies and provide their impact on operability and security. Identify and recommend to the government representatives changes to maximize network efficiency and terminal response times and script changes that will improve user interfaces and the daily operations of the LAN.

c. Identify single point of failure or other concerns to prevent host or terminal isolations. Implement government approved configuration changes to the network/LAN.

d. Perform site surveys and customer interviews required for changes to existing LAN. This action is specifically for changes relating to new requirements, moving existing LAN segments or implementing new command LAN segments.

e. Review engineering plans and site information to ensure conformance with current architecture as well as in development of future changes or enhancements to the command LAN.

f. Prepare specifications effecting material or equipment changes for implementing Government approved LAN segments to the current configuration or the new/additional LAN segments.

g. Assist government representative in determining the criteria, needs of justification for addition/enhancements to the WAN/LAN and associated hardware.

h. Prepare and submit appropriate documentation to support recommendations, evaluations, test results and report. Prepare and notify sites for implementation of new requirements.

All trip reports will be fully documented within five duty days of return. Trip reports will be provided for all Conferences, Seminars, In-Progress Reviews, Technical Develop and Engineering Studies. Trip reports will be in standard AF format and delivered to the Chief of NOSC Engineering Support for review. A sample will be provided after award.

7.0 Other Information and Special Conditions.

7.1 Special Training.

7.1.1 The Government will provide force protection training for contractor personnel and their dependents if applicable, at no cost to the contractor. The COR will inform the contractor of all Nuclear Biological Chemical (NBC) equipment and Chemical Defense Equipment (CDE) training requirements and standards. The Government will provide the contractor employees with NBC and CDE familiarization training for the performance of mission essential tasks in designated high threat countries. This training shall be equivalent to DoD civilian employee training. If required in performance of the PWS as determined by the COR, other mission related training may be required.

7.1.2 Training and job certifications of contractor employees assigned to this task order shall be performed at the contractor's own expense unless otherwise stated in the PWS, with these exceptions:

7.1.3 The Government has given prior approval for training to meet special requirements that are peculiar to the environment and/or operations.

7.1.4 Limited contractor employee training may be authorized if the Government changes hardware or software during the performance of this task order, and it is determined to be in the best interest of the Government. Once these individuals are initially trained, the contractor shall train all other individuals at the contractor's own expense.

7.1.5 The Government will not authorize contractor employees to attend seminars, symposiums, or other similar conferences unless the GSA Contracting Officer approves that attendance is mandatory for the performance of the task requirements, and it is requested by the agency to provide interface and attain knowledge necessary for the performance of this PWS.

7.1.6 In the event that the Government has approved and paid for contractor employee training, reimbursement shall not be authorized for costs associated with re-training replacement individual(s) should the employee(s) terminate from this task order. Costs that are not authorized include, but are not limited to, labor, travel, and any associated re-training expenses.

7.1.7 Arrangements will be made by HQ USAFCENT/A6 office to provide the following training to the contractor immediately prior to departure (and annually as required by Air Force or Army directives) enroute to the USCENTCOM AOR. (Location of the training may change depending upon the time frame training is required and the number of personnel scheduled to attend):

7.1.7.1 Chemical warfare defense training (CWDT).
7.1.7.2 Level 1 Antiterrorism/Force Protection Training.

7.2 Property Control.

7.2.1 The contractor shall be responsible for proper utilization and safeguarding of all government property provided for contractor use. At the end of each work period, all government facilities, equipment and materials shall be secured. Contractor employees must immediately report damage to government facilities and equipment upon discovery of such damage. Equipment found to be defective will also be reported in a timely manner, to allow for repair or replacement. These reports will be made to the QA.

7.2.2 Key Control.

The contractor shall establish and implement methods of making sure all keys issued to (or security combinations provided to) the contractor by the government are not lost or misplaced (or compromised) and are not used by unauthorized persons. The contractor shall not duplicate any keys issued by the government.

7.2.2.1 The contractor shall immediately report to the QA or contracting officer any occurrences of lost or duplicated keys or compromised combinations.

7.2.3 Lock Combinations.

The contractor shall control access to all government provided lock combinations to preclude unauthorized entry.

7.3 Conservation of Government Utilities.

The contractor shall make sure employees practice utilities conservation. The contractor shall be responsible for operating under conditions that prevent the waste of utilities.

7.4 Security Requirements.

7.4.1 Clearance Requirements: If access to classified information is a requirement at the contractor's facility, an SF 312 Non-Disclosure Agreement (NDA) initiated by the company's Facility Security Officer (FSO) is required. The contractor must possess or obtain a facility security clearance at the classification level of Secret prior to performing contract work. If the contractor does not possess a facility clearance, the government (Contracting Office) will request one. The government assumes costs and conducts security investigations for Top Secret, Secret, and Confidential facility security clearances. The contractor shall request security clearances (Submit Clearance information through DISCO to the Office of Personnel Management) for personnel requiring access to classified information within 15 days after receiving a facility clearance or, if the contractor is already cleared, within 15 days after contract award. Due to costs involved with security investigations, requests for contractor security clearances shall be kept to an absolute minimum necessary to perform contract requirements.

7.4.2 The contractor shall hire only U.S. citizens and who are suitable for holding a position of trust and able to obtain clearance for sensitive and classified information. Contract employees shall have, as a minimum, a SECRET security clearance and a TOP Secret security clearance as directed within the PWS. The highest level of security clearance required for this effort is TOP SECRET/SCI. The government will issue a DD-254 form as part of this task order.

7.4.3 The contractor must provide personnel with a variety of security clearances under this project. The minimum clearance required at task order award is a Secret clearance for all personnel. The contractor must provide personnel with Top Secret/Sensitive Compartmental Information clearance for certain government identified working environment areas. The contractor personnel will be required to handle classified materials and data aboard private or public conveyances in accordance with Air Force and Department of Defense security regulations and procedures relevant for the material. The Contractor shall be responsible for verifying employee clearance information, which shall be recorded on DD Form 254 and submitted to the Client Representative for processing through GSA and the client security office.

7.4.4 Secret Clearances. All contractor employees assigned to this task order are required to hold a valid and verifiable US Government secret clearance or higher. All personnel must hold these clearances prior to arrival at work center. The clearance must be validated and approved

by the contractor representative and CR/ACR prior to beginning work. All "unfavorable information" security check results will be reported to GSA and appropriate action will be taken. The Contractor shall bear the cost of any security clearances required for task order performance.

7.4.5 Top Secret Clearances.

7.4.5.1 Contractor employees assigned to Top Secret positions are required to hold a valid and verifiable U.S. Government Top Secret security clearance. All personnel must hold these clearances prior to arrival at work center. The clearance must be validated and approved by contactor representative and CR/ACR prior to beginning work. All "unfavorable information" security check results will be reported to GSA and appropriate action will be taken. The Contractor shall bear the cost of any security clearances required for task order performance. Internal movement or promotion of personnel within the NOSC will require personnel to have required clearances or interim prior to movement or promotion.

7.4.5.2 The contractor shall be required to have a TOP SECRET facility clearance with SECRET safeguarding capabilities not to exceed two (2) cubic feet. The contractor shall require access to Communications Security (COMSEC) Information and For Official Use Only (FOUO) Information. In performing this contract, the contractor shall receive classified documents only; perform services only; have access to classified information outside the US, Puerto Rico, US possessions and trust territories; be authorized to use the Defense Technical Information Center (DTIC); or other secondary distribution center; and have Operations Security (OPSEC) requirements. Administrative duties performed by the contractor shall not require a clearance and may require an investigation for Information Technology (IT) sensitive duties. All personnel deployed under this task order must be U.S. citizens and have a Department of Defense (DoD) security clearance of DOD SECRET and NATO SECRET unless otherwise stated in the PWS. Access to work sites is controlled.

7.4.6 Sensitive Compartmentalized Information Clearances. Contractor employees assigned to SCI positions are required to hold a valid and verifiable U.S. Government Top Secret clearance at the Sensitive Compartmentalized Information level (SCI). All personnel must hold these clearances prior to arrival at work center. TS/SCI in this solicitation means a person with a TS clearance with SCI eligibility.

Contractor employees assigned to SCI positions shall be cleared at the TS/SCI level prior to starting their performance of any work reimbursable under this task order. The contractor employer must ensure that contractor personnel are capable of timely obtaining the SCI access designation.
The clearance must be validated and approved by contractor representative and CR/ACR prior to beginning work. All "unfavorable information" security check results will be reported to GSA and appropriate action will be taken. The Contractor shall bear the cost of any security clearances required for task order performance - the contractor is allowed to provide clearances higher than those required by the contract at no cost to the government.

7.4.7 The contractor shall submit a list of all assigned support personnel for approval and distribution. Workers will not be permitted access to the work sites without appropriate information on file at the appropriate work site.

7.4.8 The host country military or civilian government officials and the DoD reserve the right to deny site access to any individual for security reasons or other sufficient cause.

7.4.9 If the contractor is notified by any Government official having security cognizance over the task order that an employee's Security Clearance has been revoked or suspended, the contractor shall notify the Government the same day as the contractor receives the notice.

7.4.10 The contractor shall provide a National Agency Check (NAC) for all contractor employees who are to be provided access to Government e-mail/internet, LAN/WAN and other Government information networks.

7.4.11 Visitor Group Security Agreement (VGSA):
The contractor shall enter into a long term visitor group security agreement if contract performance is on base for 90 days or more. This agreement shall outline how the contractor integrates security requirements for contract operations with the Air Force to ensure effective and economical operation on the installation. The agreement should address:

7.4.11.1 Security support provided by the Air Force to the contractor to include storage containers for classified information/material, use of base destruction facilities, classified reproduction facilities, use of base classified mail services, security badging, base visitor control, investigation of security incidents, base traffic regulations, the use of security forms, and conducting inspections required by DOD 5220.22-R, *Industrial Security Regulation*, and Air Force Instruction 31-601, *Industrial Security Program Management*.

7.4.11.2 Security support requiring joint Air Force and contractor coordination includes packaging classified information, mailing and receiving classified materials, implementing emergency procedures for protection of classified information, security checks, and internal security controls for protection of classified material and high value pilferable property.

7.4.11.3 On base, the long term visitor group security agreement may take the place of a Standard Practice Procedure (SPP).

7.4.12 Notifications. The contractor shall notify 20 FW/IP, 524 Nelson Ave, Shaw AFB SC 29152, 30 days before performance of the contract on Shaw AFB. The notification shall include:

- Name, address, and telephone number of company representatives.
- The contract number and contracting agency.
- The highest level of classified information which contractor employees require access to.
- The location(s) of contract performance.
- The date contract performance begins.

7.4.13 Listing of Employees. The contractor shall maintain a current listing of employees. The list shall include the employee's name, Social Security number and level of security clearance. The list shall be validated and signed by the company Facility Security Officer (FSO) and provided to the Sponsoring Agency Security Manager. An updated listing shall be provided when an employee's status or information changes. Sending a “Visit Request” through the Joint Personnel Adjudicative System (JPAS) can also fulfill this requirement.

7.4.13.1 Prior to the start of contract performance, the contractor shall identify all Key Personnel by name as identified in PWS Appendix B, to include reaffirming the Program Manager identified in the task order quote.

7.4.13.2 During the administration of the task order, any substitution of Key Personnel must be of equally or better qualified individuals as those identified in PWS Appendix B.

7.4.14 Pass and Identification Items. The contractor shall ensure the pass and identification items required for contract performance are obtained for employees and non-government owned vehicles.

7.4.15 Retrieving Identification Media. The contractor shall retrieve all identification media, including vehicle passes from employees who depart for any reason before the contract expires (e.g. terminated for cause, retirement).

7.4.16 Traffic Laws. The contractor and its employees shall comply with base and/or host nation traffic regulations.

7.4.17 Weapons, Firearms, and Ammunition. Contractor employees are prohibited from possessing weapons, firearms, or ammunition, on themselves or within their contractor-owned vehicle or privately-owned vehicle while on Shaw AFB SC or forward location.

7.4.18 For Official Use Only (FOUO). The Contractor shall comply with DoD 5400.7-R, Chapter 4, *DoD Freedom of Information Act (FOIA) Program*, requirements and Title 5 of the U.S. Code, Section 552.a. This regulation sets policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding FOUO material. The contractor shall provide training annually to the employees assigned to this task to cover at a minimum the following items: policy and procedures for the disclosure of records to the public and for marking, handling, transmitting, and safeguarding FOUO material. Annual training shall be documented and provided to the COR and GSA Contracting Office.

7.4.19 Reporting Requirements. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DoD personnel, contractor personnel, resources, and classified or unclassified defense information. Contractor employees shall be briefed by their immediate supervisor upon initial on-base assignment.

7.4.20 Physical Security. The contractor shall be responsible for safeguarding all government property and controlled forms provided for contractor use. At the end of each work period, all government facilities, equipment, and materials shall be secured.

7.4.21 Controlled/Restricted Area. The contractor shall implement local base procedures for entry to Air Force controlled/restricted areas where contractor personnel will work. An AF Form 2586, **Unescorted Entry Authorization Certificate**, must be completed and signed by the sponsoring agencies Security Manager before a Restricted Area Badge will be issued. Contractor employees must have a favorably completed National Agency Check with Written Inquiries (NACI) investigation before receiving a Restricted Area Badge. Interim access can be granted IAW AFI 31-501, *Personnel Security Program Management.*

7.4.22 Unclassified Computer Network Access. Contractors using an unclassified government computer network require completion of National Agency Check with Written Inquiries (NACI), at a minimum. If the contractor employee does not meet NACI requirements, the contractor along with the sponsoring government activity shall complete requirements for submission of a NACI investigation through the servicing security activity (20 FW/IP). The government assumes costs and conducts the NACI investigation. Personnel with a current security clearance investigation exceed NACI requirements.

7.5 Special Qualifications.

The contractor shall make sure employees have the following current and valid professional certifications before starting work under this task order and ensure any other certifications/licenses are obtained (and maintained current) as required by Host Nation regulations:

(a) A valid US driver's license
(b) A valid US passport
(c) Appropriate country visas
(d) A valid international driver's license (if required).

7.6 Privacy Act.

Work on this project may require that personnel have access to Privacy Information subject to the Privacy Act (Title 5 of the U.S. Code, Section 552.a). Reports and data shall be identified and safeguarded accordingly. Agency rules, regulations, and procedures shall be followed. The Contractor shall ensure that contractor employees assigned to this task are briefed annually on properly identifying and handling privacy act data/information.

7.7 Personal Service.

The client has determined that use of the GSA contract to satisfy this requirement is in the best interest of the government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled “Personal Services Contract”.

7.7.1 GSA will not issue orders to provide personal services. Administration and monitoring of the contractor's performance by GSA or the Client Representative shall not be so detailed or continual as to constitute supervision of contractor personnel. Government personnel may not perform any supervisory functions for contractor personnel, such as interviewing, appraising individual performance, scheduling leave or work, or directing how to perform work.

7.7.2 GSA meets the needs of its clients for information technology support through non-personal services contracts. To counter the circumstances that infer personal services and to preserve the non-personal nature of the contract, the contractor shall adhere to the following guidelines in the performance of the task.

1. Provide for direct supervision of all contract employees assigned to the task.
2. Refrain from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees with the client.
3. Ensure close communication/coordination with the GSA Information Technology Project Manager, reporting problems to the as they occur (not waiting for a monthly meeting).
4. Do not permit Government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees, terminate contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government jobs.
5. Do not assign contractor personnel to work under direct Government supervision.
6. Maintain a professional distance from Government employees.
7. Provide contractor employees with badges, if appropriate, identifying them as contractors.
8. Ensure proper communications with the Government. Technical discussion and government surveillance is acceptable, but the Government cannot tell the contractor how to do the job.
9. Assign a task leader to the task order. The task leader or alternate should be the only one who accepts tasking from the assigned Government point of contact or alternative.
10. Use work orders to document and manage the work and to define the details of the assignment and its deliverables. The Government has the right to reject the finished product or result and this does not constitute personal services.
11. When travel is required for the performance on a task, contractor personnel are only to travel as directed by their contract management.

7.8 Section 508 Compliance.

The Industry Partner shall support the Government in its compliance with Section 508 throughout the development and implementation of the work to be performed. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and

use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

The Industry Partner should review the following Web sites for additional 508 information:
http://www.section508.gov/index.cfm?FuseAction=Content&ID=12
http://www.access-board.gov/508.htm
http://www.w3.org/WAI/Resources

7.9 Past Performance Information.

The Government will provide and record Past Performance Information for services and information technology contracts that exceed $150,000.00, utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS process allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in the CPARS, so contractor's may review and comment on past performance reports submitted through the CPARS.

CPARS https://www.cpars.csd.disa.mil/
PPIRS http://www.ppirs.gov

7.10 Problem Resolution.

Contractor shall bring problems, or potential issues, affecting performance to the attention of the CR and GSA CAM as soon as possible. Verbal reports will be followed up with written reports when directed. This notification shall not relieve the Contractor of its responsibility to correct problems for which they are responsible. Contractor shall work cooperatively with the Government to resolve issues as they arise.

7.11 Closeout.

GSA Region 4 internal policies determine that as the office responsible for payment to contractors that a contract shall be closeout 90 days after the Period of Performance has ended. A request for FINAL invoice will be sent to the contractor for action, after the final invoice has been paid then a Request for Release of Claims will be sent to the contractor.

7.12 Other Direct Costs (ODC's), travel, supplies and/or materials

7.12.1 The contractor, in conjunction with the services/tasks identified in this PWS, shall be required to travel to worldwide locations, including southwest Asia to support USAFCENT NOSC requirements. The contractor may also be required to obtain supplies and/or materials for the performance of this task. Those supplies and/or materials must be incidental to and associated with the overall functions being performed through this task order. The contractor

shall abide by the requirements of the FAR in acquiring supplies and/or materials, and must maintain files in such a manner that the GSA Contracting Officer could review them upon request to ensure compliance with federal procurement regulations. Contractor teaming, partnering, and subcontracting are acceptable to provide a total solution. However, price reasonableness should always be determined prior to selecting a teammate or partner.

7.12.1.1 Anticipated ODC's are not expected to exceed the Government Reimbursable Costs budget. The below values are Estimated values for ODC.

Base Year	$ 3,065,895.20
Option Period One	$ 3,065,895.20
Option Period Two	$ 3,065,895.20
Option Period Three	$ 3,065,895.20
Option period Four	$ 3,065,895.20

7.12.2 Travel Costs.

Travel may be required to fulfill the requirements of this task. Travel will be reimbursed in accordance with the Federal Travel Regulations. Trips, numbers and types of personnel will be limited to the minimum required to accomplish the work assignment. The contractor shall use the lowest cost mode of transportation commensurate with the mission requirements and good traffic management principles. The Contractor shall ensure that the requested travel costs shall not exceed what has been authorized in the task order. Contractor incurred actual expenses resulting from Government directed travel are cost reimbursable but are limited by the Joint Travel Regulations (JTR) and must be pre-approved by the Contracting Officer's Representative and/or GSA CO or CAM.

The travel request shall be submitted to GSA for task order approval through the submission of an action memo via ITSS. The action memo must be submitted 14 work days prior to travel and must contain Contracting Officer's Representative and/or GSA CO or CAM approval, travel cost items with a total travel amount, and the total of the task order travel balance. The Contractor shall include any anticipated travel costs in the quote. While majority of the locations are listed in paragraph 2.0, all locations and duration of travel cannot be definitively established at this time. Anticipated travel and travel related costs are not expected to exceed the Government Reimbursable Costs budget.

7.12.3 Travel Related Costs.

Reimbursable Travel related costs may include costs such as pre- and post-deployment physicals, passport fees, consular fees, country sponsorship fees, cell phone expenses for Contractor personnel for Force Protection Purposes, Danger Pay, etc. The contractor shall abide by the requirements of
the FAR in acquiring travel related supplies and/or materials, and must maintain files in such a manner that the GSA Contracting Officer could review them upon request to ensure compliance with federal procurement regulations.

7.12.3.1 Anticipated travel and travel related costs are not expected to exceed the Government Reimbursable Costs budget. The below values are Estimated values for Travel:

Base Year	$ 1,080,110.11
Option Period One	$ 1,080,110.11
Option Period Two	$ 1,080,110.11
Option Period Three	$ 1,080,110.11
Option period Four	$ 1,080,110.11

7.13 Invoice and Payment Information

7.13.1 Invoice Requirements.

The invoice shall include itemized charges and other direct costs (ODCs) authorized by the COR/CO which are within scope of this task order (e.g., travel and/or training) and reflect the details specified below. An invoice for completion of each deliverable shall be electronically delivered to the Client Representative via the GSA electronic contract management system by the twentieth (20th) calendar day of the month following delivery for client and GSA acceptance. A copy of the invoice shall be attached to the associated deliverable "Acceptance Report" posted in GSA Information Technology Solution Shop (ITSS) located on the web at https://web.itss.gsa.gov/Login. The invoice shall be submitted on official company letterhead.

For travel and or training expenses, the invoiced charges shall not exceed the limit specified in the task order. No charges will be paid by the Government, which are not specifically identified in the task and approved in advance by the Government. Copies of receipts, travel vouchers, etc., completed in accordance with Government Travel Regulations shall be attached to the invoice to support the charges. Original receipts shall be maintained by the contractor and made available to Government CO, COR and or auditors upon request.

7.13.2 Payment Information.

Failure to enter an invoice into the GSA ITSS web-based system may result in a rejection. The Contractor shall provide the following payment information for GSA use. It must be an exact match with the information under the contract/task order number in the GSA ITSS Contract Registration (not the Contractor's company or individual representative's registration) as well as with the information under the Contractor's DUNS number in the System for Award Management (SAM) (http://www.sam.gov).

Mismatched information may result in rejected requests for payment.

- Company Name – Legal Business Name & DBA (Doing Business As) Name
- Mailing Address – Contact and Address Information
- Remittance Address – Remit To Address Information
- Employer's Identification Number – Federal Tax ID
- DUNS (Data Universal Numbering System)

7.13.3 Invoice Information.

- Invoice Number – must not include any special characters; ITSS and the invoice must match.
- ACT Number from GSA Form 300, Block 4
- GSA Task Order Number – must match ITSS
- Contract Number from GSA Form 300, Block 3
- Point of Contact and Phone Number
- Charges, identified by deliverable or line item(s), with a narrative description of the service performed.
- Labor, travel and training, and other charges must be broken out in accordance with the contract Prompt Payment Discount, if offered.
- Total Invoice Amount – must match the acceptance information posted in ITSS; cannot exceed the current task order ceiling
- Total cumulative task order amount

7.13.4 Invoice Submittal.

A copy of the invoice must be posted in the GSA ITSS web-based Order Processing System (http://it-solutions.gsa.gov) or future equivalent. The Client Representative/COR and GSA Contract Specialist must approve the invoice in ITSS prior to payment.

The original invoice must be submitted to the GSA Finance Service Center. This shall be done electronically to the finance center web site (http://www.finance.gsa.gov).

The invoice information posted in ITSS must match the invoice information submitted to GSA's Finance Center to initiate a receiving report. The payment information must be a three-way match ITSS, GSA Finance Center, and the System for Award Management (SAM) for the invoice to be successfully processed for payment.

7.13.5 Final Invoice/Task Order Closeout.

The invoice for final payment must be so identified and submitted within 60 days from task order completion. No invoices shall be submitted after the FINAL invoice is submitted.. The Contractor can Mark with the word FINAL (even if it is a zero amount). l. After the final invoice has been paid the Contractor shall furnish a completed and signed Release of Claims to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

7.14 Records/Data.

All data and data rights associated with this effort will be property of the U.S. Government. See DFAR clause 252.227-71 and 252.227-72. Contractors are subject to the same non-disclosure
agreements (NDA) conditions agreed on by the NOSC while working with other commercial companies and vendors. The Government has unlimited rights to all deliverables of this task order to include intellectual property rights of all software developed in support of the tasks defined within the PWS. The contractor shall develop, maintain, and sustain software data packages as required by the PWS with no less than Government Purpose Rights and the Government shall retain ownership of all source code and scripts. Anticipated costs associated with intellectual property rights shall be coordinated and pre-approved by the Government COR in writing prior to the costs being incurred. The contractor shall provide invoices/receipts to the COR for all allowable costs associated with intellectual property rights.

8.0 Government Estimates and Required Qualifications/Certifications

8.1 Reserved

8.2 Estimated Government Workload: **See Appendix F.**

8.3 TDY Travel Estimates: See Appendix G. Any hours above an 80 hour, two week work period will be charged as Labor Hours. Below is an estimate of the number of TDY's per FTE with an estimated amount of Labors that has historically been used in the past.

9.0 Federal Acquisition Regulations and Supplements, and Executive Orders

All applicable contract clauses, provisions, and terms and conditions from the **GSA Alliant GWAC** are hereby *incorporated* into this task order.

This task order incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting officer will make their full text available. Also the full text of a clause may be accessed electronically at this/these address(es):

FAR website:	http://www.acquisition.gov/far/
DFARS/AFFARS website:	http://www.farsite.hill.af.mil/
GSAM website:	http://www.acquisiton.gov/comp/gsam/gsam.html

Clauses. All applicable provisions and clauses identified in the GSA Alliant GWAC are applicable to this task order.

CLAUSES INCORPORATED BY REFERENCE

52.203-11	Certification And Disclosure Regarding Payments To Influence Certain Federal Transactions	SEP 2007
52.212-1	Instructions to Offerors--Commercial Items	APR 2014
52.212-4 Alt 1	Contract Terms and Conditions – Commercial Items	MAY 2014
52.217-5	Evaluation Of Options	JUL 1990
52.222-17	Nondisplacement of Qualified Workers	May 2014
52.228-3	Workers' Compensation Insurance (Defense Base Act)	JUL 2014
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	APR 1992
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2007
252.204-7000	Disclosure of Information	DEC 1991
252.204-7003	Control Of Government Personnel Work Product	APR 2003
252.204-7004 Alt	Central Contractor Registration (52.204-7) Alternate A	DEC 2008
252.203-7005	Representation Relating to Compensation of Former DOD Officials	NOV 2011
252.205-7000	Provision of Information to Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting with Firms That are Owned or Controlled by the Government of a Terrorist Country	DEC 2006
252.215-7007	Notice of Intent to Resolicit	JUN 2012
252.215-7008	Only one Offer	OCT 2013
252.225-7002	Qualifying Country Sources As Subcontractors	OCT 2006
252.225-7005	Identification of Expenditures in the United States	JUN 2005
252.225-7006	Quarterly Reporting of Actual Contract Performance Outside the United States	OCT 2010
252.225-7012	Preference For Certain Domestic Commodities	NOV 2008
252.225-7013	Duty-Free Entry	SEP 2004
252.225-7021	Trade Agreements	DEC 1991
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	MAR 1998
252.237-7023	Continuation of Essential Contractor Services	OCT 2010
252.237-7024	Notice of Continuation of Essential Contractor Services	OCT 2010
252.239-7000	Protection Against Compromising Emanations	JUN 2004
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008

252.243-7001	Pricing Of Contract Modifications	MAR 2008
252.243-7002	Requests for Equitable Adjustment	JUN 2011
252.225-7040	Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States.	
252.225.7043	Antiterrorism/Force Protection for Defense Contractors Outside The United States	

CLAUSES INCORPORATED BY FULL TEXT

FAR 52.217-8, Option to Extend Services (Nov 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder **shall not exceed 6 months**. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

(End of Clause)

FAR 52.217-9, Option to Extend the Term of the Contract (Mar 2000)
(a) The Government may extend the term of this contract by written notice to the Contractor **within 30 days**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60 days** before the contract expires. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, **shall not exceed 5 (five) years**.

(End of Clause)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

Deviation 2012-00007
Class Deviation-Additional Responsibility Matters When Using Fiscal Year 2012 Funds.

252.209-7998 Representation Regarding Conviction of a Felony Criminal Violation under any Federal or State Law.

REPRESENTATION REGARDING CONVICTION OF A FELONY CRIMINAL VIOLATION UNDER ANY FEDERAL OR STATE LAW (DEVIATION 2012-00007) (DATE 2012)

(a) In accordance with section 514 of Division H of the Consolidated Appropriations Act, 2012, none of the funds made available by that Act may be used to enter into a contract with any corporation that was convicted of a felony criminal violation under any Federal or State law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.

(b) The Offeror represents that it is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal or State law within the preceding 24 months.

End of Provision

Deviation 2012-00004
Class Deviation— Prohibition Against Contracting With Corporations That Have an Unpaid Delinquent Tax liability or a Felony Conviction under Federal Law

DFARS 252.232-7007 Limitation of Government's Obligation (May 2006)
(a) Contract line item(s) * through * are incrementally funded. For these item(s), the sum of $ * of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise

the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract	$ _____
(month) (day), (year)	$ _____
(month) (day), (year)	$ _____
(month) (day), (year)	$ _____

5352.215-9000 Facility Clearance

As prescribed in 5315.209, insert in Section L a provision substantially the same as the following provision:

FACILITY CLEARANCE (MAY 1996)

The offeror must possess, or acquire prior to award of a contract, a facility clearance equal to the highest classification stated on the Contract Security Classification Specification (DD Form 254) attached to this solicitation.

5352.223-9000 Elimination of Use of Class I Ozone Depleting Substances (ODS)

As prescribed in 5323.804, insert the following clause in solicitations and contracts:

ELIMINATION OF USE OF CLASS I OZONE DEPLETING SUBSTANCES (ODS) (APR 2003)

(a) Unless the requiring activity has obtained prior Senior Acquisition Official (SAO) approval, contractors may not:

(1) Provide any service or product with any specification, standard, drawing, or other document that requires the use of a Class I ODS in the test, operation, or maintenance of any system, subsystem, item, component, or process; or

(2) Provide any specification, standard, drawing, or other document that establishes a test, operation, or maintenance requirement that can only be met by use of a Class I ODS.

[Note: This prohibition does not apply to manufacturing.]

(b) For the purposes of Air Force policy, the following products that are pure (i.e., they meet the relevant product specification identified in AFI 32-7086) are Class I ODSs:

(1) Halons: 1011, 1202, 1211, 1301, and 2402;

(2) Chlorofluorocarbons (CFCs): CFC-11, CFC-12, CFC-13, CFC-111, CFC-112, CFC-113, CFC-114, CFC-115, CFC-211, CFC-212, CFC-213, CFC-214, CFC-215, CFC-216, and CFC-217, and the blends R-500, R-501, R-502, and R-503; and

(3) Carbon Tetrachloride, Methyl Chloroform, and Methyl Bromide.

[NOTE: Material that uses one or more of these Class I ODSs as minor constituents do not meet the Air Force definition of a Class I ODS.]

(c) The requiring activity has obtained SAO approval to permit the contractor to use the following Class I ODS(s):

Class I ODS/ Application or Use/Quantity (lbs.) per contract period of performance

[*List each Class I ODS, its applications or use and the approved quantities for use throughout the length of the contract. If "None," so state.*]

(d) The offeror/contractor is required to notify the contracting officer if any Class I ODS that is not specifically listed above is required in the test, operation, or maintenance of any system, subsystem, item, component, or process.

(End of clause)

5352.223-9001 Health and Safety on Government Installations

As prescribed in 5323.9001, insert the following clause in solicitations and contracts:

HEALTH AND SAFETY ON GOVERNMENT INSTALLATIONS (JUN 1997)

(a) In performing work under this contract on a Government installation, the contractor shall:

(1) Comply with the specific health and safety requirements established by this contract;

(2) Comply with the health and safety rules of the Government installation that concern related activities not directly addressed in this contract;

(3) Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of contractor and Government personnel performing or in any way coming in contact with the performance of this contract; and

(4) Take such additional immediate precautions as the contracting officer may reasonably require for health and safety purposes.

(b) The contracting officer may, by written order, direct Air Force Occupational Safety and Health (AFOSH) Standards and/or health/safety standards as may be required in the performance of this contract and any adjustments resulting from such direction will be in accordance with the Changes clause of this contract.

(c) Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the contracting officer, shall be grounds for termination of this contract in accordance with the Default clause of this contract.

(End of clause)

5352.242-9000 Contractor Access to Air Force Installations

As prescribed in 5342.490-1, insert a clause substantially the same as the following clause in solicitations and contracts:

CONTRACTOR ACCESS TO AIR FORCE INSTALLATIONS (AUGUST 2007)

(a) The contractor shall obtain base identification and vehicle passes, if required, for all contractor personnel who make frequent visits to or perform work on the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on the installation.

(b) The contractor shall submit a written request on company letterhead to the contracting officer listing the following: contract number, location of work site, start and stop dates, and names of employees and subcontractor employees needing access to the base. The letter will also specify the individual(s) authorized to sign for a request for base identification credentials or vehicle passes. The contracting officer will endorse the request and forward it to the issuing base pass and registration office or security police for processing. When reporting to the registration office, the authorized contractor individual(s) should provide a valid driver's license, current vehicle registration, valid vehicle insurance certificate, and [*insert any additional requirements to comply with local security procedures*] to obtain a vehicle pass.

(c) During performance of the contract, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials and vehicle passes for any employee who no longer requires access to the work site.

(d) When work under this contract requires unescorted entry to controlled or restricted areas, the contractor shall comply with *[insert any additional requirements to comply with AFI 31-101, Volume 1, The Air Force Installation Security Program, and AFI 31-501, Personnel Security Program Management,]* citing the appropriate paragraphs as applicable.

(e) Upon completion or termination of the contract or expiration of the identification passes, the prime contractor shall ensure that all base identification passes issued to employees and subcontractor employees are returned to the issuing office.

(f) Failure to comply with these requirements may result in withholding of final payment.

(End of clause)

5352.242-9001 Common Access Cards (CAC) for Contractor Personnel

As prescribed in 5342.490-2, insert a clause substantially the same as the following clause in solicitations and contracts:

COMMON ACCESS CARDS (CAC) FOR CONTRACTOR PERSONNEL (AUG 2004)

(a) For installation(s)/location(s) cited in the contract, contractors shall ensure Common Access Cards (CACs) are obtained by all contract or subcontract personnel who meet one or both of the following criteria:

(1) Require logical access to Department of Defense computer networks and systems in either:

(i) the unclassified environment; or

(ii) the classified environment where authorized by governing security directives.

(2) Perform work, which requires the use of a CAC for installation entry control or physical access to facilities and buildings.

(b) Contractors and their personnel shall use the following procedures to obtain CACs:

(1) Contractors shall provide a listing of personnel authorized a CAC to the contracting officer. The contracting officer will provide a copy of the listing to the government representative in the local organization designated to authorize issuance of contractor CACs (i.e., "authorizing official").

(2) Contractor personnel on the listing shall each complete and submit a DD Form 1172-2 or other authorized DoD electronic form to the authorizing official. The authorizing official will verify the applicant's name against the contractor's listing and return the DD Form 1172-2 to the contractor personnel.

(3) Contractor personnel will proceed to the nearest CAC issuance workstation (usually the local Military Personnel Flight (MPF) with the DD Form 1172-2 and appropriate documentation to support their identification and/or citizenship. The CAC issuance workstation will then issue the CAC.

(c) While visiting or performing work on installation(s)/location(s), contractor personnel shall wear or prominently display the CAC as required by the governing local policy.

(d) During the performance period of the contract, the contractor shall:

(1) Within 7 working days of any changes to the listing of the contract personnel authorized a CAC, provide an updated listing to the contracting officer who will provide the updated listing to the authorizing official;

(2) Return CACs in accordance with local policy/directives within 7 working days of a change in status for contractor personnel who no longer require logical or physical access;

(3) Return CACs in accordance with local policy/directives within 7 working days following a CACs expiration date; and

(4) Report lost or stolen CACs in accordance with local policy/directives.

(e) Within 7 working days following completion/termination of the contract, the contractor shall return all CACs issued to their personnel to the issuing office or the location specified by local policy/directives.

(f) Failure to comply with these requirements may result in withholding of final payment.

APPENDIX A

Contractor Key Personnel and Qualifications

The contractor's key personnel to include: position/title, work experience, education/clearance, certifications, and training shall be incorporated here as Appendix B prior to start of task order performance. A recommended format is provided below, however the offeror may organize the information as deemed appropriate to meet the requirements of PWS Section 2.0. This Appendix will be considered proprietary and not releasable under the Freedom of Information Act.

Key Position/Title	Work Experience	Education/Clearance	Certifications	Training	Other Information Provided by the Offeror

APPENDIX B

ACRONYM LIST

A

AB-	Air Base
ACC-	Air Combat Command
ACO-	Air Coordination Order
ADSI-	Air Defense System Integrator
AFB-	Air Force Base
AF-	Air Force
AFI-	Air Force Instruction
AFMAN-	Air Force Manual
AFPD-	Air Force Policy Directive
ALMSS-	Automated Logistics Management Support System
AMIC-	Acquisition Management and Integration Center
AOC-	Air and Space Operations Center
AOR-	Area of Responsibility
AQL-	Assurance Quality Level
ATO-	Air Tasking Order
ATOMS-	Automated Technical Order Management System

B

BS-	Bachelor of Science

C

C2	Command and Control
C4ISR-	Command, Control, Communications, Computers, Intelligence, Surveillance/Reconn
C&A	
CA/CRL	Custodian Authorization Custody Receipt Listing
CaM-	Capacity Management
CAOC-	Combined Air and Space Operations Center
CBT-	Computer Based Training
CCAA-	Citrix Certified Advanced Administrator
CCEE-	Citrix Certified Enterprise Engineer
CCNA-	Cisco Certified Network Associate
CCNP-	Cisco Certified Network Professional
CDE-	Chemical Defense Equipment
CENTCOM-	Central Command
CENTRIX-	Combined Enterprise Regional Information Exchange
CFACC-	Combined Forces Air Component Commander

CFP-	Communication Focal Point
CISA-	Certified Information Systems Auditor
CISSP-	Certified Information Systems Security Professional
CM-	Configuration Management
CO-	Contracting Officer
COMSEC-	Communications Security
CONUS-	Continental U.S.
COR-	Contracting Officer Representative
COR-	Contracting Officer Representative
COTS/GOTS-	Commercial Off-the-Shelf/Government Off-the-Shelf
CPS-	Contractor Performance System
CSA	Communication Support Activity

D

DAA	Designated Accreditation Authority
DBA-	Database Administrator
DBMS-	Database Management System
DICAP-	Department of Defense Information Assurance Certification and Accreditation Proce
DISA-	Defense Information Systems Agency
DISCO-	Defense Industrial Security Clearance Office
DFC-	Deployed Forward Commander
DoD-	Department of Defense
DoDD-	Department of Defense Directive
DoDI-	Department of Defense Instruction
DoDM-	Department of Defense Manual
DUNS-	Data Universal Numbering System

E

ETIMS-	Enhanced Technical Information Management System

F

FAR-	Federal Acquisition Regulation
FOIA-	Freedom of Information Act
FOUO-	For Official Use Only
FSO-	Facility Security Officer
FW-	Fighter Wing

G

GFE-	Government Furnished Equipment
GSA-	General Service Administration

H

HAZMAT-	Hazardous Material

I

IA-	Information Assurance
IAO-	Information Assurance Officer
IAW-	In Accordance With
IDS-	Intrusion Detection System
IMDS-	Integrated Management Data System
IP-	Internet Protocol
ISM-	Information Security Manager
ISSO	Information System Support Office
IT-	Information Technology
ITIL-	Information Technology Infrastructure Library
ITSS-	Information Technology Systems and Services

J

JADOCS-	Joint Air Defense Operations Center System
JPAS-	Joint Personnel Adjudicative System
JRE-	Joint Range Extender
JTF-	Joint Task Force
JTR-	Joint Travel Regulation
JWICS-	Joint Worldwide Intelligence Communications System

K

KSA-	Knowledge, skills and abilities

L

LAN-	Local Area Network
LMR-	Land Mobile Radio
LOA-	Letter of Authorization

M

MCP-	Microsoft Certified Professional
MCSA WINDOWS 7 OR ABOVE-	Microsoft Certified Solution Associate
MCSE - MESSAGING CERTIFICATION-	Microsoft Certified System Engineer
MLS-	Multi-Level Security
MSL-	Master Station Log
MS-SQL	Microsoft Structured Query Language

N

NAC-	National Agency Check
NACI-	National Agency Check with Written Inquiries
NBC-	Nuclear Biological Chemical
NCC-	Network Control Center
NDA-	Non-Disclosure Agreement
NIH-	National Institute of Health
NOSC-	Network Operations Service Center

O

O&M-	Operations and Maintenance
OCONUS-	Outside the Continental U.S.
ODC-	Other Direct Charges
ODR-P-	Office of the Defense Representative-Pakistan
OPSEC-	Operations Security
OSSA-	Oracle Solaris System Administrator

P

PKI-	Public Key Infrastructure
PM-	Preventative Maintenance
POA&M-	Plan of Action and Milestones
PoP	Period of Performance
PPIRS-	Past Performance Information Retrieval System
PWS-	Performance Work Statement

Q

QA-	Quality Assurance
QAE-	Quality Assurance Evaluator
QASP-	Quality Assurance Surveillance Plan
QCP-	Quality Control Plan

R

RCA-	Root Cause Analysis
RHCE-	Red Hat Certified Engineer
RHCSA-	Red Hat Certified System Administrator
RM-	Remedial Maintenance
ROM-	Rough Order of Magnitude

S

SBSS-	Standard Base Supply System
SCR-	Software Change Request
SOC-	Security Operations Center
SOP-	Standard Operating Procedures
SPIN-C	Special Instructions - Communications
SPOT-	Synchronized Predeployment & Operational Tracker
SPP-	Standard Practice Procedure

T

TBMCS-	Theater Battle Management Communication System
TIA-	Technology Industry Association
TO-	Task Order
TRS-	Tactical Receive Suite

U

USAF	United States Air Force
USAFCENT-	United States Air Forces Central

V

VCP-	VMware Cert Professional

W

WAN- Wide Area Network
WAVE- Wide Area Voice Environment

Appendix C: Government Furnished Equipment & Materials, NOSC Training Lab

Qty	Part Number	Description
12	C2951-VSEC-CUBE/K9	C2951 UC SEC CUBE Bundle, PVDM3-32, UC SEC Lic, FL-CUBEE-25
12	FL-GK-2951	Gatekeeper Feature License -2951 platform
12	MEM-2951-512U4GB	512MB to 4GB DRAM Upgrade (2 2GB DIMM) for Cisco 2951 ISR
12	MEM-CF-256U4GB	256MB to 4GB Compact Flash Upgrade for Cisco 1900,2900,3900
12	PWR-2921-51-POE	Cisco 2921/2951 AC Power Supply with Power Over Ethernet
12	CAB-AC	AC Power Cord (North America), C13, NEMA 5-15P, 2.1m
12	HWIC-16A	16-Port Async HWIC
12	HWIC-4T	4-Port Serial HWIC
12	S2951UK9-15204M	Cisco 2951 IOS UNIVERSAL
12	NM-HDV2-2T1/E1	IP Communications High-Density Digital Voice NM with 2 T1/E1
12	VWIC2-2MFT-T1/E1	2-Port 2nd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1
12	VIC2-4FXO	Four-port Voice Interface Card - FXO (Universal)
12	VIC3-4FXS/DID	Four-Port Voice Interface Card - FXS and DID
12	SL-29-DATA-K9	Data License for Cisco 2901-2951
12	SM-ES3G-24-P	Enhcd EtherSwitch, L2/L3, SM, 24 GE, POE
12	SL-29-UC-K9	Unified Communication License for Cisco 2901-2951
12	ISR-CCP-EXP	Cisco Config Pro Express on Router Flash
12	SL-29-SEC-K9	Security License for Cisco 2901-2951
24	CAB-HD8-ASYNC	High Density 8-port EIA-232 Async Cable
12	SL-29-IPB-K9	IP Base License for Cisco 2901-2951
48	CAB-SS-232MT	RS-232 Cable, DTE Male to Smart Serial, 10 Feet
12	FL-CUBEE-25	Unified Border Element Enterprise License - 25 sessions
12	PI-MSE-PRMO-INSRT	Insert, Packout - PI-MSE
12	PVDM3-32U256	PVDM3 32-channel to 256-channel factory upgrade
12	SM-NM-ADPTR	Network Module Adapter for SM Slot on Cisco 2900, 3900 ISR
12	FL-29-HSEC-K9	U.S. Export Restriction Compliance license for 2921/2951
12	FL-CME	Cisco Communications Manager Express License
12	FL-CME-SRST-25	Communication Manager Express or SRST - 25 seat license
48	CAB-SS-232FC	RS-232 Cable, DCE Female to Smart Serial, 10 Feet
12	ISM-SRE-300-K9	Internal Services Module (ISM) with Services Ready Engine
24	WS-C3850-24P-E	Cisco Catalyst 3850 24 Port PoE IP Services
48	CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors
24	C3850-NM-4-1G	Cisco Catalyst 3850 4 x 1GE Network Module
24	S3850UK9-33SE	CAT3850 Universal k9 image
24	STACK-T1-1M	1M Type 1 Stacking Cable
24	PWR-C1-715WAC/2	715W AC Config 1 Secondary Power Supply
24	CAB-SPWR-30CM	Catalyst 3750X Stack Power Cable 30 CM
24	PWR-C1-715WAC	715W AC Config 1 Power Supply
12	CP-8961-C-K9=	Cisco UC phone 8961, Charcoal, Standard handset
1	N20-Z0001	Cisco Unified Computing System
3	N20-C6508	UCS 5108 Blade Svr AC Chassis/0 PSU/8 fans/0 fabric extender
48	N20-BBLKD	UCS 2.5 inch HDD blanking panel
48	UCSB-HS-01-EP	CPU Heat Sink for UCS B200 M3 and B420 M3
6	UCS-IOM-2208XP	UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)
12	UCSB-PSU-2500ACDV	2500W Platinum AC Hot Plug Power Supply - DV
12	CAB-C19-CBN	Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors
3	N20-FW012	UCS Blade Server Chassis FW Package 2.2
3	N01-UAC1	Single phase AC power module for UCS 5108
3	N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis
24	N20-FAN5	Fan module for UCS 5108
3	UCSB-5108-PKG-HW	UCS 5108 Packaging for chassis with half width blades.
4	UCSB-B200-M3	UCS B200 M3 Blade Server w/o CPU, memory, HDD, mLOM/mezz
48	N1K-VSG-UCS-BUN	Nexus 1000V Adv Edition for vSphere Paper License Qty 1
48	N1K-VLEM-UCS-1	Nexus 1000V License Paper Delivery (1 CPU) for bundles

Appendix D: Government Furnished Equipment & Materials to support Contractor Site Lab.

SYSTEMS			
Racks and Equipment			
Line #	**Product Number**	**Product Description**	**Qty**
1	224-4934	Dell 4220 42U Rack with Doors and Side Panels, Ground Ship NOT for AK / HI	12
2	220-4932	Dell 4220 42U Rack with Doors and No Side Panels, Ground Ship NOT for AK / HI	2
3	330-3601	Rack Interconnect Kit, PS to PS, Customer Install	12
4	A0333377	AP7540 Rack PDU, Basic, Zero U, 20A, 208V, (20)C13 & (4)C19	24
5	SUA3000RMT2U	APC Smart-UPS 3000VA USB & Serial RM 2U 208V	24
6	A2521511	Raritan T1900 LCD KVM Drawer	6
7	A1175068	Raritan 32-port Dominion KX II-432 KVM-over-IP Switch	6
8	A1229346	16-Port Dominion KX2-416 KVM-Over-IP Switch	10
Miscellaneous Equipment			
9	D2CIM-DVUSB-64PA	Raritan Enhanced USB CIM required for virtual media, 64 pack	2
10	313-9669	External Trayload Optical Multi-Format CD/DVD USB Drive	2
11	A0137220	Generic 1U Rails	1
12	A0168851	Generic 2U Rails	1
13	2331	5' C14 to C13 PDU to Server Cable	200
14	2337	6' C14 to C13 PDU to Server Cable	100
15	2302	7' C14 to C13 PDU to Server Cable	60
Temperature Monitor and Probes			
16	731-1000	Sensatronics EM 1	1
17	600-1088-50	Temp/RH Probe w/ 50-Ft Cable	4
Network Time Servers			
18	383041001	NTPSYNC II/ANT/US PWR CORD	2
Boundary Firewalls			
19	FWE - S5032G	CS-USAF MFE Firewall Enterprise 2150F Appl	4
20	FWES-5032-ARMAG	CS-USAFMFE Firewall Enterprise 2150 C D E 1Yr GL plusNBD	4
Web Proxy Servers			
21	SG900-10B-PR	Blue Coat SG900-10, Proxy Edition	4
22	SL131Y-SG900-10-PR	Standard Support, 24x7 L1-L3 Software Only, 1 YR, SG900-10-PR	4
23	HNBDS1Y-SG900-10-PR	Next Business Day, Support, Hardware Only, 1 YR, SG900-10-PR	4
24	SG900-10	SSL License, SG900-10	4
25	AV1400-A	Blue Coat AV1400-A	2
26	SL131Y-AV1400-A	Standard Support, 24X7 L1-L3 Software Only, 1 YR, AV1400-A	2
27	HNBDS1Y-AV1400-A	Next Business Day, Support, Hardware Only, 1 YR, AV140-A	2
Active Directory Domain Controllers			

29	Dell Power Edge R620 (225-2108) Base Unit	Each Dell Power Edge R620 (225-2108) Base Unit - is configured per specifications contained below. Each R620 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	6
		PowerEdge R620 (225-2108)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1787)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4668)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (953-0165)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (953-0166)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (953-0167)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R620 Shipping - 4/8 Drive Chassis (331-4761)	1
		iDRAC7 Enterprise (421-5339)	1
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		Cable for Mini PERC Cards for Chassis with up to 8 Hard Drives (331-4823)	1
		Chassis with up to 8 Hard Drives and 3 PCIe Slots (342-3666)	1
		Bezel-4/8 Drive Chassis (318-1431)	1
		Power Saving Dell Active Power Controller (330-5116)	1
		RAID 0 for H710P/H710/H310 (1-10 HDDs) (331-4223)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Intel Xeon E5-2609 2.40GHz,10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W, Max Mem 1066MHz (317-9590)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		DIMM Blanks for Systems with 2 Processors (317-8688)	1
		Intel Xeon E5-2609 2.40GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W (317-9606)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		4GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width (317-5135)	4
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	6
		Electronic System Documentation and OpenManage DVD Kit (331-4513)	1
		DVD+/-RW, SATA, Internal (318-1391)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4765)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1

		CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
		CFI Bypass EIDO (364-7502)	1
		CFI,Information, Hotspare,Hard Drive,Factory Install (361-8968)	1
		CFI,Information SKU to Set RAID1 Container on First Two Hard Drives and RAID5 on Other Hard Drives,Factory Ins (361-7117)	1
		CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
		CFI Titan Code for Image SI#s (364-1848)	1
		CFI,Information,Hard Drive,Install Increasing Order,Factory Install (361-1722)	1
		CFI,Fee,Integration,Tier1,RAID (366-4243)	1
		CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
		CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
		CFI Routing SKU (365-0257)	1
		CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
		CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
		AMC,CFS,UID,LBL (490-0375)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		Enterprise Messaging Servers	
30	Dell Power Edge R520 (225-2980) Base Unit	Each Dell Power Edge R520 (225-2980) Base Unit - is configured per specifications contained below. Each R520 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	6
		PowerEdge R520 (225-2980)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (939-9437)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-9677)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (951-6203)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (951-6208)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (951-6237)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R520 Shipping (331-7113)	1
		Risers with up to 4 x16 PCIe Slots (331-7118)	1
		On-Board Broadcom 5720 Dual Port 1GBE (430-4715)	1
		iDRAC Port Card (421-5340)	1
		iDRAC7 Enterprise (421-6085)	1
		3.5" Chassis with up to 4 or 8 Hard Drives (318-2065)	1
		SAS Cable for Hardware RAID (331-7108)	1
		Bezel (318-1375)	1
		RAID 5 for H710P/H710/H310 (3-8 HDDs) (331-7103)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Heat Sink,PowerEdge (317-9826)	1

		Intel Xeon E5-2440 2.40GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W (319-0023)	1
		Heat Sink,PowerEdge (317-9826)	1
		Intel Xeon E5-2440 2.40GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W (319-0032)	1
		4GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width (317-5135)	6
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 3.5in Hot-plug Hard Drive (342-2078)	8
		Electronic System Documentation and OpenManage DVD Kit for R520 (331-7116)	1
		DVD+/-RW, SATA, INTERNAL (313-9090)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4433)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Distribution Board for Hot Plug Power Supplies (331-7112)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1
		Americas Merge Center Service (490-0000)	1
		AMC,CFS,UID,LBL (490-0375)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Enterprise Personnel Alert System	
31	Dell Power Edge R620 (225-2108) Base Unit	Each Dell Power Edge R620 (225-2108) Base Unit - is configured per specifications contained below. Each R620 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	6
		PowerEdge R620 (225-2108)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1787)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4668)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (953-0165)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (953-0166)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (953-0167)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R620 Shipping - 4/8 Drive Chassis (331-4761)	1
		iDRAC7 Enterprise (421-5339)	1
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		Cable for Mini PERC Cards for Chassis with up to 8 Hard Drives (331-4823)	1
		Chassis with up to 8 Hard Drives and 3 PCIe Slots (342-3666)	1
		Bezel-4/8 Drive Chassis (318-1431)	1
		Power Saving Dell Active Power Controller (330-5116)	1
		RAID 0 for H710P/H710/H310 (1-10 HDDs) (331-4223)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Intel Xeon E5-2609 2.40GHz,10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W, Max Mem 1066MHz (317-9590)	1
		Heat Sink for PowerEdge R620 (331-4762)	1

		DIMM Blanks for Systems with 2 Processors (317-8688)	1
		Intel Xeon E5-2609 2.40GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W (317-9606)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		4GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width (317-5135)	4
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	6
		Electronic System Documentation and OpenManage DVD Kit (331-4513)	1
		DVD+/-RW, SATA, Internal (318-1391)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4765)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1
		CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
		CFI Bypass EIDO (364-7502)	1
		CFI,Information, Hotspare,Hard Drive,Factory Install (361-8968)	1
		CFI,Information SKU to Set RAID1 Container on First Two Hard Drives and RAID5 on Other Hard Drives,Factory Ins (361-7117)	1
		CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
		CFI Titan Code for Image SI#s (364-1848)	1
		CFI,Information,Hard Drive,Install Increasing Order,Factory Install (361-1722)	1
		CFI,Fee,Integration,Tier1,RAID (366-4243)	1
		CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
		CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
		CFI Routing SKU (365-0257)	1
		CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
		CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		AMC,CFS,UID,LBL (490-0375)	1
Enterprise Desktop Management			
32	Dell Power Edge R720 (225-2133) Base Unit	Each Dell Power Edge R720 (225-2133) Base Unit - is configured per specifications contained below. Each R720 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	4
		PowerEdge R720 (225-2133)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-2678)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (939-2768)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (951-7896)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (951-7904)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (951-7918)	1
		On-Site Installation Declined (900-9997)	1

	Proactive Maintenance Service Declined (926-2979)	1
	Keep Your Hard Drive, 3 Year (983-6402)	1
	PowerEdge R720 Shipping (331-4437)	1
	Risers with up to 4, x8 PCIe Slots + 2, x16 PCIe Slot (331-4439)	1
	iDRAC7 Enterprise (421-5339)	1
	Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
	2.5" Chassis with up to 8 + 8 Hard Drives and 2 Controllers (331-4613)	1
	Bezel (318-1375)	1
	Power Saving Dell Active Power Controller (330-5116)	1
	RAID 0/Unconfigured RAID for Dual H710P (1 + 1-7 + 1-8 HDDs) (331-4406)	1
	PERC H710P Integrated RAID Controller, 1GB NV Cache (342-3530)	1
	PERC H710P Integrated RAID Controller, 1GB NV Cache (342-3531)	1
	Intel Xeon E5-2609 2.40GHz,10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W, Max Mem 1066MHz (317-9590)	1
	Heat Sink for PowerEdge R720 and R720xd (331-4508)	1
	DIMM Blanks for Systems with 2 Processors (317-8688)	1
	Intel Xeon E5-2609 2.40GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W (317-9606)	1
	Heat Sink for PowerEdge R720 and R720xd (331-4508)	1
	4GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width (317-5135)	4
	1333 MHz RDIMMs (331-4422)	1
	Performance Optimized (331-4428)	1
	300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	8
	No System Documentation, No OpenManage DVD Kit (310-5171)	1
	DVD+/-RW, SATA, INTERNAL (313-9090)	1
	ReadyRails Sliding Rails With Cable Management Arm (331-4433)	1
	Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
	Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
	No Operating System (420-6320)	1
	No Media Required (421-5736)	1
	CFI Bypass EIDO (364-7502)	1
	CFI Titan Code for Image SI#s (364-1848)	1
	CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
	CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
	CFI,Fee,Integration,Tier1,RAID (366-4243)	1
	CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
	CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
	CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
	CFI,Information,Raid,Custom, Factory Install (364-7651)	1
	CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
	CFI Routing SKU (365-0257)	1
	CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
	Americas Merge Center Service (490-0000)	1
	AMC,CFS,UID,LBL (490-0375)	1

		Enterprise Trouble Ticket Management System	
33	LP757.0.0.00	BMC Remedy AR System Server (Note: Contract Number 21486)	1
34	LA179.0.0.00	BMC Remedy AR System Fixed 1-Pk Lsn	5
35	LA172.0.0.00	BMC Remedy AR System Flt 1-Pk Lsn	10
		Enterprise Centralized Database Servers	
36	Dell Power Edge R620 (225-2108) Base Unit (Note: 1 HBA per server; 64GB RAM)	Each Dell Power Edge R620 (225-2108) Base Unit - is configured per specifications contained below. Each R620 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	4
		PowerEdge R620 (225-2108)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1787)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4668)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (953-0165)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (953-0166)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (953-0167)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R620 Shipping - 4/8 Drive Chassis (331-4761)	1
		iDRAC7 Enterprise (421-5339)	1
		Qlogic 2562 Dual Channel 8Gb Optical Fibre Channel HBA PCIe, Low Profile (342-3547)	1
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		Cable for Mini PERC Cards for Chassis with up to 8 Hard Drives (331-4823)	1
		Chassis with up to 8 Hard Drives and 3 PCIe Slots (342-3666)	1
		Bezel-4/8 Drive Chassis (318-1431)	1
		Power Saving Dell Active Power Controller (330-5116)	1
		RAID 0 for H710P/H710/H310 (1-10 HDDs) (331-4223)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, Max Mem 1333MHz (317-9595)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		DIMM Blanks for Systems with 2 Processors (317-8688)	1
		Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W (317-9609)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		8GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x4 Data Width (317-9644)	8
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	6
		Electronic System Documentation and OpenManage DVD Kit (331-4513)	1
		DVD+/-RW, SATA, Internal (318-1391)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4765)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1

		No Media Required (421-5736)	1
		CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
		CFI Bypass EIDO (364-7502)	1
		CFI Routing SKU (365-0257)	1
		CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
		CFI,Information SKU to Set RAID1 Container on First Two Hard Drives and RAID5 on Other Hard Drives,Factory Ins (361-7117)	1
		CFI,Information,Hard Drive,Install Increasing Order,Factory Install (361-1722)	1
		CFI Titan Code for Image SI#s (364-1848)	1
		CFI,Information, Hotspare,Hard Drive,Factory Install (361-8968)	1
		CFI,Fee,Integration,Tier1,RAID (366-4243)	1
		CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
		CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
		CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
		CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		AMC,CFS,UID,LBL (490-0375)	1
		Enterprise Backup System	
37	Dell Power Edge R620 (225-2108) Base Unit	Each Dell Power Edge R620 (225-2108) Base Unit - is configured per specifications contained below. Each R620 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	2
		PowerEdge R620 (225-2108)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1787)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4668)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (953-0165)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (953-0166)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (953-0167)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R620 Shipping - 4/8 Drive Chassis (331-4761)	1
		iDRAC7 Enterprise (421-5339)	1
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		Cable for Mini PERC Cards for Chassis with up to 8 Hard Drives (331-4823)	1
		Chassis with up to 8 Hard Drives and 3 PCIe Slots (342-3666)	1
		Bezel-4/8 Drive Chassis (318-1431)	1
		Performance BIOS Setting (330-3492)	1
		RAID 1+RAID 5 for H710P/H710/H310 (2 + 3-8 HDDs) (331-4237)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Intel Xeon E5-2650 2.00GHz, 20M Caches, 8.0GT/s QPI, Turbo, 8C, 95W, Max Mem 1600MHZ (317-9252)	1
		Heat Sink for PowerEdge R620 (331-4762)	1

		Intel Xeon E5-2650 2.00GHz, 20M Caches, 8.0GT/s QPI, Turbo, 8C, 95W (317-8458)	1
		DIMM Blanks for Systems with 2 Processors (317-8688)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		2GB RDIMM, 1600MT/s, Low Volt, Single Rank, x8 Data Width (319-1809)	8
		1600 MHZ RDIMMS (331-4424)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gps 2.5in Hot-plug Hard Drive (342-2240)	2
		1TB 7.2K RPM Near-Line SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2001)	6
		Electronic System Documentation and OpenManage DVD Kit (331-4513)	1
		DVD+/-RW, SATA, Internal (318-1391)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4765)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1
		AMC,CFS,UID,LBL (490-0375)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		Enterprise Collaboration System	
38	Dell Power Edge R620 (225-2108) Base Unit (Note: 1 dual port HBA per server; 64GB RAM)	Each Dell Power Edge R620 (225-2108) Base Unit - is configured per specifications contained below. Each R620 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	4
		PowerEdge R620 (225-2108)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1787)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4668)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (953-0165)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (953-0166)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (953-0167)	1
		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R620 Shipping - 4/8 Drive Chassis (331-4761)	1
		iDRAC7 Enterprise (421-5339)	1
		Qlogic 2560 Single Channel 8Gb Optical Fibre Channel HBA PCIe, Low Profile (342-3546)	2
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		Cable for Mini PERC Cards for Chassis with up to 8 Hard Drives (331-4823)	1
		Chassis with up to 8 Hard Drives and 3 PCIe Slots (342-3666)	1
		Bezel-4/8 Drive Chassis (318-1431)	1
		Power Saving Dell Active Power Controller (330-5116)	1
		RAID 0 for H710P/H710/H310 (1-10 HDDs) (331-4223)	1
		PERC H710 Integrated RAID Controller, 512MB NV Cache (342-3529)	1
		Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, Max Mem 1333MHz (317-	1

		9595)	
		Heat Sink for PowerEdge R620 (331-4762)	1
		DIMM Blanks for Systems with 2 Processors (317-8688)	1
		Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W (317-9609)	1
		Heat Sink for PowerEdge R620 (331-4762)	1
		8GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x4 Data Width (317-9644)	8
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	6
		Electronic System Documentation and OpenManage DVD Kit (331-4513)	1
		DVD+/-RW, SATA, Internal (318-1391)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4765)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
		Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1
		CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
		CFI Bypass EIDO (364-7502)	1
		CFI Routing SKU (365-0257)	1
		CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
		CFI,Information SKU to Set RAID1 Container on First Two Hard Drives and RAID5 on Other Hard Drives,Factory Ins (361-7117)	1
		CFI,Information,Hard Drive,Install Increasing Order,Factory Install (361-1722)	1
		CFI Titan Code for Image SI#s (364-1848)	1
		CFI,Information, Hotspare,Hard Drive,Factory Install (361-8968)	1
		CFI,Fee,Integration,Tier1,RAID (366-4243)	1
		CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
		CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
		CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
		CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		AMC,CFS,UID,LBL (490-0375)	1
		Enterprise Virtual Server System	
39	Dell Power Edge R820 (225-2607) Base Unit	Each Dell Power Edge R720 (225-22607) Base Unit - is configured per specifications contained below. Each R720 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	12
		PowerEdge R820 (225-2607)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (936-1997)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-4938)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (951-3226)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (951-3227)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (951-3254)	1

		On-Site Installation Declined (900-9997)	1
		Proactive Maintenance Service Declined (926-2979)	1
		Keep Your Hard Drive, 3 Year (983-6402)	1
		PowerEdge R820 Shipping (331-6156)	1
		iDRAC7 Enterprise (421-5339)	1
		QLogic 8262, Dual Port 10Gb SFP+, Converged Network Adapter, Low Profile (430-4403)	2
		Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
		2.5" Chassis with up to 8 Hard Drives (331-6157)	1
		Bezel (318-1375)	1
		Power Saving Dell Active Power Controller (330-5116)	1
		RAID 5 for H710p, H710, H310 Controllers (331-5686)	1
		PERC H710 Adapter RAID Controller, 512MB NV Cache, Full Height (342-4048)	1
		2x Intel Xeon E5-4620 2.20GHz, 16M Cache, 7.2GT/s QPI, Turbo, 8 Core, 95W, Max Mem 1333MHz (317-9327)	1
		Heat Sink for PowerEdge R820 (331-6161)	1
		DIMM Blanks for Systems up to 4 Processors (317-9332)	1
		Upgrade to Four Intel Xeon E5-4620 2.20GHz, 16M Cache, 7 2GT/s QPI, Turbo, 8 Core, 95W (317-9335)	1
		Heat Sink for PowerEdge R820 (331-6161)	1
		PWA for PowerEdge R820 (331-6162)	1
		16GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x4 Data Width (319-0111)	8
		1333 MHz RDIMMs (331-4422)	1
		Performance Optimized (331-4428)	1
		300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	3
		Electronic System Documentation and OpenManage DVD Kit for R820 (331-6872)	1
		DVD+/-RW, SATA, INTERNAL (313-9090)	1
		ReadyRails Sliding Rails With Cable Management Arm (331-4433)	1
		Dual, Hot-plug, Redundant Power Supply (1+1), 1100W (331-4607)	1
		Power Cord, NEMA 5-15P to C13, 15 amp, wall plug, 10 feet / 3 meter (310-8509)	2
		No Operating System (420-6320)	1
		No Media Required (421-5736)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
		Americas Merge Center Service (490-0000)	1
		AMC,CFS,UID,LBL (490-0375)	1
Enterprise ISO Servers			
40	Dell Power Edge R720 (225-2133) Base Unit	Each Dell Power Edge R720 (225-2133) Base Unit - is configured per specifications contained below. Each R720 unit has part numbers for the components listed at the end of each description column cell and required component quantities in the QTY Cell.	2
		PowerEdge R720 (225-2133)	1
		Dell Hardware Limited Warranty Plus On Site Service Extended Year (939-2678)	1
		Dell Hardware Limited Warranty Plus On Site Service Initial Year (939-2768)	1
		Dell ProSupport Plus. For tech support, visit www.dell.com/prosupport/regionalcontacts (951-2015)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, 2 Year Extended (951-7896)	1
		ProSupport Plus: Mission Critical 4-Hour 7x24 On-Site Service with Emergency Dispatch, Initial Year (951-7904)	1
		ProSupport Plus: 7x24 HW/SW Tech Support and Assistance, 3 Year (951-7918)	1

	On-Site Installation Declined (900-9997)	1
	Proactive Maintenance Service Declined (926-2979)	1
	Keep Your Hard Drive, 3 Year (983-6402)	1
	PowerEdge R720 Shipping (331-4437)	1
	Risers with up to 4, x8 PCIe Slots + 2, x16 PCIe Slot (331-4439)	1
	iDRAC7 Enterprise (421-5339)	1
	Broadcom 5720 QP 1Gb Network Daughter Card (430-4418)	1
	2.5" Chassis with up to 8 + 8 Hard Drives and 2 Controllers (331-4613)	1
	Bezel (318-1375)	1
	Power Saving Dell Active Power Controller (330-5116)	1
	RAID 0/Unconfigured RAID for Dual H710P (1 + 1-7 + 1-8 HDDs) (331-4406)	1
	PERC H710P Integrated RAID Controller, 1GB NV Cache (342-3530)	1
	PERC H710P Integrated RAID Controller, 1GB NV Cache (342-3531)	1
	Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W, Max Mem 1333MHz (317-9595)	1
	Heat Sink for PowerEdge R720 and R720xd (331-4508)	1
	DIMM Blanks for Systems with 2 Processors (317-8688)	1
	Intel Xeon E5-2640 2.50GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C, 95W (317-9609)	1
	Heat Sink for PowerEdge R720 and R720xd (331-4508)	1
	4GB RDIMM, 1333 MT/s, Low Volt, Dual Rank, x8 Data Width (317-5135)	4
	1333 MHz RDIMMs (331-4422)	1
	Performance Optimized (331-4428)	1
	300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive (342-2240)	8
	No System Documentation, No OpenManage DVD Kit (310-5171)	1
	DVD+/-RW, SATA, INTERNAL (313-9090)	1
	ReadyRails Sliding Rails With Cable Management Arm (331-4433)	1
	Dual, Hot-plug, Redundant Power Supply (1+1), 750W (331-4605)	1
	Power Cord, C13 to C14, PDU Style, 12 Amps, 4 meter, Qty 1 (330-3152)	2
	No Operating System (420-6320)	1
	No Media Required (421-5736)	1
	CFI,Information,Raid,Custom, Factory Install (364-7651)	1
	CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
	CFI Routing SKU (365-0257)	1
	CFI Titan Code for Image SI#s (364-1848)	1
	CFI Bypass EIDO (364-7502)	1
	CFI,Software,Image,Generic, Factory,Domestic,2,Factory Install (364-7618)	1
	CFI,Fee,Integration,Tier1,RAID (366-4243)	1
	CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
	CFI Fee,RU Image,Stat, 200,SV (366-4236)	1
	CFI,Information,VPE,IMAGE, PROCESS,Factory Install (372-6268)	1
	CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
	CUSTOM ProSupport - Federal On-Site IT Support (937-5129)	1
	Americas Merge Center Service (490-0000)	1

		AMC,CFS,UID,LBL (490-0375)	1
		Enterprise Centralized Database Reporter Servers	
41	VNX5700SPEF	EMC VNX5700	2
	FSTS-V57	FAST Suite for VNX5700	2
	VSPMXGFCOEOPA	Dual port FCoE module	4
	VNX6GSDAE15PF	VNX 55/75 15X3.5 6GB SAS PRIMARY DAE F I	2
	VNXSPS1KWF	VNX57/75 1.2KW SPS 15/25 DRV VLT DAE-F I	2
	VNX6GSDAE15F	VNX 15X3.5 IN 6GB SAS EXP DAE-FLD INST	16
	FLVXVS6F-200	200GB FAST CACHE FLASH	10
	VX-VS15-600	600GB 15K 520BPS 6GB SAS 3.5 CARRIER	162
	VX-VS07-030	3.5 IN 3T 7200RPM DISK DRV FOR 6GSDAE-15	90
	V-VX-V30010	3.5 300G 10K VAULT PCK 6GSDAE/DPE	2
	MSAS-MSAS-2M	One pr of Mini-SAS - Mini-SAS 2M cables	2
	VNX57-KIT	DOCUMENTATION KIT FOR VNX5700	2
	M-PRESW-001	PREMIUM SOFTWARE SUPPORT	2
	WU-PREHW-001	PREMIUM HARDWARE SUPPORT - WARR UPG	2
	UNIB-V57	UNISPHERE FOR BLOCK FOR A VNX 5700	2
	VNXOE-57	VNX OE LICENSE MODEL FOR VNX5700	2
	VNXOECAPTB	VNX OE PER TB HI CAP-VNX5500;5700;7500	272
	VNXOEPERFTB	VNX OE PER TB PER FOR VNX5500;5700;7500	98
	PS-BAS-DSKRT3	DISK RETENTION; 3 YEAR	11
		NETWORKS	
		Riverbed Equipment	
Line #	**Product Number**	**Product Description**	**Qty**
42	LIC-CXA-1555-H	License Steelhead CXA 1555-H, 100 Mbps, 6000 conn	4
43	CXA-01555-B020	Steelhead CXA 1555 B020 with RiOS	4
44	MNT-GLD-CXA-01555	Steelhead CXA 1555 Gold Support	4
45	MNT-HER-1U-CX	Disc/Memory Support-xx55 CX15555	4
		Tier 1	
46	WS-C3850-24T-E	Cisco Catalyst 3850 24 Port Data IP Services	12
47	CAB-C15-CBN	Cabinet Jumper Power Cord 250 VAC 13A C14-C15 Connectors	24
48	PWR-C1-350WAC/2	350W AC Config 1 SecondaryPower Supply	12
49	S3850UK9-32-0SE	CAT3850 UNIVERSAL	12
50	C3850-NM-4-1G	Cisco Catalyst 3850 4 x 1GE Network Module	12
51	STACK-T1-50CM	50CM Type 1 Stacking Cable	12
52	CAB-SPWR-30CM	Catalyst 3750X Stack Power Cable 30 CM	12
53	PWR-C1-350WAC	350W AC Config 1 Power Supply	12
54	CISCO3945-HSEC+/K9	VPN ISM module HSEC bundles for 3945 ISR platform	6
55	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	12
56	CAB-SS-530AMT	RS-530A Cable DTE Male to Smart Serial 10 Feet	48
57	C3900-SPE150/K9	Cisco Services Performance Engine 150 for Cisco 3945 ISR	6

58	ISM-VPN-39	3DES/AES/SUITE-B VPN Encryption module	6
59	SL-39-IPB-K9	IP Base License for Cisco 3925/3945	6
60	3900-FANASSY	Cisco 3925/3945 Fan Assembly (Bezel included)	6
61	ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	6
62	SL-39-SEC-K9	Security License for Cisco 3900 Series	6
63	S39UK9-15204M	Cisco 3925-3945 IOS UNIVERSAL	6
64	SL-39-DATA-K9	Data License for Cisco 3900 Series	6
65	SM-ES3G-16-P	Enhcd EtherSwitch L2/L3 SM 16GE POE	6
66	SL-ES3G-16-IPS	IP Services License Upgrade 16 Port GE ES3 EtherSwitch	6
67	HWIC-4T	4-Port Serial HWIC	12
68	FL-39-HSEC-K9	U.S. Export Restriction Compliance license for 3900 series	6
69	MEM-3900-1GU4GB	1GB to 4GB DRAM Upgrade (2GB+2GB) for Cisco 3925/3945 ISR	6
70	MEM-CF-256U4GB	256MB to 4GB Compact Flash Upgrade for Cisco 190029003900	6
71	PWR-3900-AC	Cisco 3925/3945 AC Power Supply	6
72	PWR-3900-AC/2	Cisco 3925/3945 AC Power Supply (Secondary PS)	6
		Access Switches	
73	WS-C3850-48P-E	Cisco Catalyst 3850 48 Port PoE IP Services	30
74	CAB-TA-NA	North America AC Type A Power Cable	60
75	PWR-C1-1100WAC/2	1100W AC Config 1 Secondary Power Supply	30
76	S3850UK9-32-0SE	CAT3850 UNIVERSAL	30
77	C3850-NM-4-10G	Cisco Catalyst 3850 4 x 10GE Network Module	30
78	STACK-T1-50CM	50CM Type 1 Stacking Cable	30
79	CAB-SPWR-30CM	Catalyst 3750X Stack Power Cable 30 CM	30
80	PWR-C1-715WAC	715W AC Config 1 Power Supply	30
81	WS-C3750X-24S-E	Catalyst 3750X 24 Port GE SFP IP Services	5
82	CAB-3KX-AC	AC Power Cord for Catalyst 3K-X (North America)	10
83	C3KX-PWR-715WAC/2	Catalyst 3K-X 715W AC Secondary Power Supply	5
84	S375XVK9T-15002SE	CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR	5
85	C3KX-NM-10G	Catalyst 3K-X 10G Network Module option PID	5
86	CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	5
87	CAB-SPWR-30CM	Catalyst 3750X Stack Power Cable 30 CM	5
88	C3KX-PWR-350WAC	Catalyst 3K-X 350W AC Power Supply	5
		External/Internal CSIDS	
89	IPS-4360-K9	IPS 4360 with SW 8 GE data + 1 GE mgmt AC Power	2
90	IPS-4360-AC-PWR	IPS 4360 AC power supply	2
91	SF-IPS-4300-7.1-K9	IPS 4345 and 4360 Software Version 7.1	2
92	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2
93	IPS-4360-AC-PWR	IPS 4360 AC power supply	2
94	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	2
		Cisco Datacenter	
95	N7K-C7009-B2S2E-R	Nexus7009 Bundle(Chassis 2xSUP2E 5xFAB2) No Power Supplies	4
96	N7K-SUP2E	Nexus 7000 - Supervisor 2 EnhancedIncludes 8GB USB Flash	4
97	N7K-USB-8GB	Nexus 7K USB Flash Memory - 8GB (Log Flash)	4

98	N7K-F248XP-25E	Nexus 7000 F2-Series 48 Port 1/10G (SFP+) Enhanced	4
99	N7K-FCOEF248XP	FCoE License for Nexus 7000 48-port 10G SFP+ (F2)	4
100	N7K-F248XP-25E	Nexus 7000 F2-Series 48 Port 1/10G (SFP+) Enhanced	4
101	N7K-FCOEF248XP	FCoE License for Nexus 7000 48-port 10G SFP+ (F2)	4
102	N7KS2K9-61	Cisco NX-OS Release 6.1 for SUP2	4
103	N7K-C7009-SBUN-P1	Inc LANADVTRSEL2DCNMDCNMSANMPLSSANXL - Promotion	4
104	DCNM-N7K-K9-SBUN	DCNM for LAN Enterprise License for one Nexus 7000 Chassis	4
105	DCNM-SANN7KK9-SBUN	DCNM for SAN Advanced Edition for Nexus 7000	4
106	N7K-ADV1K9-SBUN	Nexus 7000 Advanced LAN Enterprise License (VDC CTS ONLY)	4
107	N7K-C7009-XL-SBUN	Nexus 7009 Scalable Feature License	4
108	N7K-EL21K9-SBUN	Nexus 7000 Enhanced Layer 2 License (FabricPath)	4
109	N7K-LAN1K9-SBUN	Nexus 7000 LAN Enterprise License (L3 protocols)	4
110	N7K-MPLS1K9-SBUN	Nexus 7000 MPLS License	4
111	N7K-SAN1K9-SBUN	Nexus 7000 SAN Enterprise License	4
112	N7K-TRS1K9-SBUN	Nexus 7000 Transport Services License	4
113	N7K-VDC1K9	Nexus 7000 Incremental VDC license (+4 VDC per license)	4
114	N7K-SUP2E	Nexus 7000 - Supervisor 2 EnhancedIncludes 8GB USB Flash	4
115	N7K-USB-8GB	Nexus 7K USB Flash Memory - 8GB (Log Flash)	4
116	N7K-M148GT-11L	Nexus 7000 - 48 Port 10/100/1000 Module with XL option	4
117	N7K-M224XP-23L	Nexus 7000 M2-Series 24 Port 10GE with XL Option (req. SFP+)	4
118	N7K-M148GS-11L	Nexus 7000 - 48 Port GE Module with XL Option (req. SFP)	4
119	N7K-C7009-FAB-2	Nexus 7000 - 9 Slot Chassis - 110Gbps/Slot Fabric Module	20
120	N7K-AC-6.0KW	Nexus 7000 - 6.0KW AC Power Supply Module	8
121	CAB-AC-C6K-TWLK	Power Cord 250Vac 16A twist lock NEMA L6-20 plug US	16
122	N7K-C7009-FD-MB	Nexus 7009 Front Door Kit	4
123	DCNM-PAK	DCNM Advanced License Kit for Nexus and MDS switches	4
124	N2K-C2248PQF	Nexus 2248PQ with (8 FET-40G) or (4 FET-40G and 16 FET-10G)	12
125	N2K-F40G-F10G	N2K Uplink option FET-40G to FET-10G	12
126	CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	24
127	FET-10G	10G Line Extender for FEX	192
128	FET-40G	40G Line Extender for FEX	48
129	N2200-PAC-400W-SN	N2200-PAC-400W Power Supply - Service Specific	24
130	NXA-FAN-30CFM-F-SN	Service Specific - Fan	48
131	N2248PQ-FA-BUN	Standard airflow pack: N2K-C2248PQ-10GE 2AC PS 4Fan	12
132	N2K-C2248TF-E	Nexus 2248TP-E with 8 FET choice of airflow/power	12
133	N2K-F10G-F10G	N2K Uplink option FET-10G to FET-10G	12
134	CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	24
135	FET-10G	10G Line Extender for FEX	96
136	N2248TP-E-FA-BUN	Standard Airflow pack:N2K-C2248TP-E-1GE 2 AC PS 1Fan	12
137	N1K-VLCPU-04=	Nexus 1000V Adv Edition for vSphere Paper License Qty 4	6
138	VSG-VL-CPU-04	VSG Paper CPU License Qty 4	6
139	VSG-VL-CPU-01	VSG Paper CPU License Qty 1	24
140	VNMC2X-VSG-01	VNMC 2.X VSG management one CPU Physical Delivery	24
141	N1K-VLCPU-01	Nexus 1000V Paper CPU License Qty 1	24

Voice			
142	N20-Z0001	Cisco Unified Computing System	2
143	N20-C6508	UCS 5108 Blade Svr AC Chassis/0 PSU/8 fans/0 fabric extender	4
144	N20-FW011	UCS Blade Server Chassis FW Package 2.1	4
145	UCSB-B200-M3	UCS B200 M3 Blade Server w/o CPU, memory, HDD, mLOM/mezz	12
146	UCS-CPU-E5-2690	2.90 GHz E5-2690/135W 8C/20MB Cache/DDR3 1600MHz	24
147	UCS-MR-1X162RY-A	16GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	96
148	UCSB-MLOM-40G-01	Cisco UCS VIC 1240 modular LOM for M3 blade servers	12
149	UCSB-MLOM-PT-01	Cisco UCS Port Expander Card (mezz) for VIC 1240 modular LOM	12
150	N20-BBLKD	UCS 2.5 inch HDD blanking panel	24
151	UCSB-HS-01-EP	CPU Heat Sink for UCS B200 M3 and B420 M3	24
152	N1K-VSG-UCS-BUN	Nexus 1000V Adv Edition for vSphere Paper License Qty 1	24
153	N1K-VLEM-UCS-1	Nexus 1000V License Paper Delivery (1 CPU) for bundles	24
154	VSG-VLEM-UCS-1	VSG License Paper Delivery (1 CPU) for bundles	24
155	UCS-IOM-2208XP	UCS 2208XP I/O Module (8 External, 32 Internal 10Gb Ports)	8
156	N01-UAC1	Single phase AC power module for UCS 5108	4
157	N20-CAK	Accessory kit for UCS 5108 Blade Server Chassis	4
158	N20-CBLKB1	Blade slot blanking panel for UCS 5108/single slot	20
159	N20-FAN5	Fan module for UCS 5108	32
160	UCSB-PSU-2500ACPL	2500W Platinum AC Hot Plug Power Supply for UCS 5108 Chassis	16
161	CAB-C19-CBN	Cabinet Jumper Power Cord, 250 VAC 16A, C20-C19 Connectors	16
162	UCS-FI-6248UP	UCS 6248UP 1RU Fabric Int/No PSU/32 UP/ 12p LIC	4
163	SFP-10G-SR	10GBASE-SR SFP Module	16
164	UCS-ACC-6248UP	UCS 6248UP Chassis Accessory Kit	4
165	UCS-PSU-6248UP-AC	UCS 6248UP Power Supply/100-240VAC	8
166	N10-MGT011	UCS Manager v2.1	4
167	CAB-AC-L620-C13	AC Power Cord, NEMA L6-20 - C13, 2M/6.5ft	8
168	UCS-FAN-6248UP	UCS 6248UP Fan Module	8
169	UCS-FI-DL2	UCS 6248 Layer 2 Daughter Card	4
170	UCS-FI-E16UP	UCS 6200 16-port Expansion module/16 UP/ 8p LIC	4
171	UCSC-C220-M3S	UCS C220 M3 SFF w/o CPU mem HDD PCIe PSU w/ rail kit	4
172	UCS-CPU-E5-2690	2.90 GHz E5-2690/135W 8C/20MB Cache/DDR3 1600MHz	8
173	UCS-MR-1X162RY-A	16GB DDR3-1600-MHz RDIMM/PC3-12800/dual rank/1.35v	32
174	UCS-HDD300GI2F105	300GB 6Gb SAS 15K RPM SFF HDD/hot plug/drive sled mounted	32
175	UCSC-CMA1	Reversible Cable Management Arm for C220C22C24 servers	4
176	CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	8
177	UCSC-PSU-650W	650W power supply for C-series rack servers	8
178	UCSC-RAID-11-C220	Cisco UCS RAID SAS 2008M-8i Mezz Card for C220 (0/1/10/5/50)	4
179	UCSC-PCIE-CSC-02	Cisco VIC 1225 Dual Port 10Gb SFP+ CNA	4
180	UCSC-HS-C220M3	Heat Sink for UCS C220 M3 Rack Server	8
181	UCSC-PCIF-01H	Half height PCIe filler for UCS	4
182	UCSC-RAIL1	Rail Kit for C220 C22 C24 rack servers	4
183	N2K-C2232PF	Nexus 2232PP with 16 FET choice of airflow/power	4
184	N2K-F10G-F10G	N2K Uplink option FET-10G to FET-10G	4

185	CAB-C13-C14-2M	Power Cord Jumper C13-C14 Connectors 2 Meter Length	8
186	FET-10G	10G Line Extender for FEX	64
187	N2232PP-FA-BUN	Standard airflow pack: N2K-C2232PP-10GE 2AC PS 1Fan	4
188	C3945E-CME-SRST/K9	3945E UC Bundle w/ PVDM3-64 FL-CME-SRST-25 UC License PA	8
189	FL-LMR	LMR Feature License	8
190	MEM-3900-1GU2GB	1GB to 2GB DRAM Upgrade (1GB+1GB) for Cisco 3925/3945 ISR	8
191	MEM-CF-256U4GB	256MB to 4GB Compact Flash Upgrade for Cisco 190029003900	8
192	PWR-3900-AC	Cisco 3925/3945 AC Power Supply	8
193	PWR-3900-AC/2	Cisco 3925/3945 AC Power Supply (Secondary PS)	8
194	CAB-AC	AC Power Cord (North America) C13 NEMA 5-15P 2.1m	16
195	C3900-SPE250/K9	Cisco Services Performance Engine 250 for Cisco 3945E ISR	8
196	FL-CME-SRST-25	Communication Manager Express or SRST - 25 seat license	8
197	SL-39-IPB-K9	IP Base License for Cisco 3925/3945	8
198	SM-NM-ADPTR	Network Module Adapter for SM Slot on Cisco 2900 3900 ISR	16
199	FL-CME	Cisco Communications Manager Express License	8
200	FL-CME-SRST-25	Communication Manager Express or SRST - 25 seat license	8
201	SL-39-UC-K9	Unified Communication License for Cisco 3900 Series	8
202	3900-FANASSY	Cisco 3925/3945 Fan Assembly (Bezel included)	8
203	ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	8
204	S39EUK9-15204M	Cisco 3925-3945 SPE IOS UNIVERSAL	8
205	UCS-E140S-M1/K9	UCS-ESingleWide4Cor CPU2x8G SD1x8GB UDIMM1-2 HDD	8
206	E100-SD-8G	8 GB SD Card for SingleWide and DoubleWide UCS-E	8
207	E100S-MEM-UDIMM8G	8GB 1333MHz VLP UDIMM/PC3-10600 2R for SinglWde UCS-E	8
208	E100S-MEM-UDIMM8G	8GB 1333MHz VLP UDIMM/PC3-10600 2R for SinglWde UCS-E	8
209	E100S-HDD-SAS900G	900 GB SAS hard disk drive for SingleWide UCS-E	16
210	DISK-MODE-RAID-1	Configure hard drives as RAID 1 (Mirror)	8
211	UCS-E140S-M1/K9	UCS-ESingleWide4Cor CPU2x8G SD1x8GB UDIMM1-2 HDD	8
212	E100-SD-8G	8 GB SD Card for SingleWide and DoubleWide UCS-E	8
213	E100S-MEM-UDIMM8G	8GB 1333MHz VLP UDIMM/PC3-10600 2R for SinglWde UCS-E	8
214	E100S-MEM-UDIMM8G	8GB 1333MHz VLP UDIMM/PC3-10600 2R for SinglWde UCS-E	8
215	E100S-HDD-SAS900G	900 GB SAS hard disk drive for SingleWide UCS-E	16
216	DISK-MODE-RAID-1	Configure hard drives as RAID 1 (Mirror)	8
217	NM-HDV2-2T1/E1	IP Communications High-Density Digital Voice NM with 2 T1/E1	8
218	VIC2-4FXO	Four-port Voice Interface Card - FXO (Universal)	8
219	NM-HDV2-2T1/E1	IP Communications High-Density Digital Voice NM with 2 T1/E1	8
220	VIC3-4FXS/DID	Four-Port Voice Interface Card - FXS and DID	8
221	VWIC3-4MFT-T1/E1	4-Port 3rd Gen Multiflex Trunk Voice/WAN Int. Card - T1/E1	24
222	PVDM3-64U256	PVDM3 64-channel to 256-channel factory upgrade	8
223	FL-CUBEE-100-RED	Unified Border Element Ent Lic 100 Sessions Redundancy	8
224	FL-GK-3945	Gatekeeper Feature License -3945 platform	8
225	FL-VXML-12	VoiceXML Feature License Up To 12 Sessions	8
226	CP-8945-K9=	Cisco Unified Phone 8945 Phantom Grey Standard Handset	100
227	CP-9971-C-CAM-K9=	Cisco UC Phone 9971 Charcoal Std Hndst with Camera	10
228	CP-7937G	Cisco UC Conference Station 7937 Global	8

229	SW-CCM-UL-7937	CUCM 3.x or 4.x RTU lic. for single Conf. Station 7937	8
230	CP-PWR-CUBE-3	IP Phone power transformer for the 7900 phone series	8
231	CP-PWR-CORD-NA	Power Cord North America	8
232	CP-7937-MIC-KIT	Microphone Kit for 7937	8
233	CP-PWR-CUBE-4=	IP Phone power transformer for the 89/9900 phone series	110
234	CP-PWR-CORD-NA=	Power Cord North America	110
235	CP-CKEM-C=	Cisco Unified IP Color Key Expansion Module Charcoal	10
		Cable	
236	MADVJ-1	1 Meter LC to SC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	20
237	MADVJ-2	2 Meter LC to SC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	40
238	MADVJ-3	3 Meter LC to SC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	20
239	MADVG-15	15 Meter LC to SC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	2
240	MADVS-1	1 Meter LC to LC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	60
241	MADVS-2	2 Meter LC to LC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	40
242	MADVS-3	3 Meter LC to LC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	100
243	MADVS-15	15 Meter LC to LC Fiber Patch Cords (Multimode 50/125 - Full Duplex) Riser Jacket	2
244	S8DVS-1	1 Meter LC to LC Fiber Patch Cords (Single Mode - Full Duplex)	60
245	S8DVS-2	2 Meter LC to LC Fiber Patch Cords (Single Mode - Full Duplex)	50
246	S8DVS-3	3 Meter LC to LC Fiber Patch Cords (Single Mode - Full Duplex)	70
247	S8DVJ-1	1 Meter LC to SC Fiber Patch Cords (Single Mode - Full Duplex)	60
248	S8DVJ-2	2 Meter LC to SC Fiber Patch Cords (Single Mode - Full Duplex)	50
249	S8DVJ-3	3 Meter LC to SC Fiber Patch Cords (Single Mode - Full Duplex)	90
250	S8DVG-3	3 Meter SC to SC Fiber Patch Cords (Single Mode - Full Duplex)	30
251	570-120-010	3Meter /10ft RJ45 to RJ45 Patch Cord, non-plenum, Solid Core (GREEN)	500
252	570-130-010	3Meter /10ft RJ45 to RJ45 Patch Cord, non-plenum, Solid Core (RED)	500
253	570-120-003	1 Meter RJ45 to RJ45 Patch Cord, non-plenum, Solid Core (GREEN)	150
254	570-130-003	1 Meter RJ45 to RJ45 Patch Cord, non-plenum, Solid Core (Red)	150
255	PC5ENP4P24-GN-R-BER-PV	1000ft box of Cat5e, Non Plenum Cable, Solid Core (Green)	1
256	PC5ENP4P24-RD-R-BER-PV	1000ft box of Cat5e, Non Plenum Cable, Solid Core (Red)	1
257	5-554720-3	RJ-45 Connectors	1200
258	569875-4	Hooded RJ-45 Boots (Green)	800
259	569875-3	Hooded RJ-45 Boots (Red)	400
260	CCH-04U	Chassis, 4U high with 4 CCH-CP12-91 LC/LC panels. Each panel has 6 duplex LC connections.	2
261	CCH-03U	Chassis, 3U high with 4 CCH-CP12-91 LC/LC panels. Each panel has 6 duplex LC connections.	2
262	CCH-01U	Chassis, 1U high with 1 CCH-CP12-91 LC/LC panel. Each panel has 6 duplex LC connections	12

263	CCH-CP12-E4	6 port, duplex, LC panel, 12 total strands	60
264	17437	Coupler, singlemode, duplex SC / SC	100
265	R6F011	Coupler, multimode, duplex, SC / SC	100
266	RFQLN16	MM, 50/125, 12 connectors, Plenum LC / LC, 2 meters = 6 feet	2
267	RFQLN17	MM, 50/125, 12 connectors, Plenum LC / LC, 2.5 meters = 8 feet	2
268	RFQLN18	MM, 50/125, 12 connectors, Plenum LC / LC, 3.1 meters = 10 feet	2
269	RFQLN19	MM, 50/125, 12 connectors, Plenum LC / LC, = 12 feet	2
270	RFQLN20	MM, 50/125, 12 connectors, Plenum LC / LC, = 14 feet	2
271	RFQLN21	MM, 50/125, 12 connectors, Plenum LC / LC, = 16 feet	2
		Optics	
272	GLC-LH-SMD=	1000BASE-LX/LH SFP transceiver module MMF/SMF 1310nm DOM	200
273	GLC-SX-MMD=	1000BASE-SX SFP transceiver module MMF 850nm DOM	100
274	SFP-GE-T=	1000BASE-T SFP (NEBS 3 ESD)	350
275	SFP-10G-SR=	10GBASE-SR SFP Module	50
276	SFP-10G-LR=	10GBASE-LR SFP Module	50
277	SFP-H10GB-CU1M=	10GBASE-CU SFP+ Cable 1 Meter	50
278	SFP-H10GB-CU1-5M=	10GBASE-CU SFP+ Cable 1.5 Meter	50
279	SFP-H10GB-CU2M=	10GBASE-CU SFP+ Cable 2 Meter	75
280	SFP-H10GB-CU2-5M=	10GBASE-CU SFP+ Cable 2.5 Meter	100
281	SFP-H10GB-CU3M=	10GBASE-CU SFP+ Cable 3 Meter	150
282	SFP-H10GB-ACU7M=	Active Twinax cable assembly 7m	50
283	SFP-H10GB-ACU10M=	Active Twinax cable assembly 10m	25
284	QSFP-4X10G-AC7M=	QSFP to 4xSFP10G Active Copper Splitter Cable 7m	25
		Miscellaneous Equipment	
285	SU2200RMXLTNET	APC Smart-UPS 2200 Input: L6-20P/\Output: (1) L6-20R + (2) L6-30R + (2) 5-15R	4
286	LPS500A-MM-LC	BLACKBOX Multimode to Ethernet POE Media Converter	30
287	901053	Data Ready - Network Tools Kit - BLACK, RJ 45 Termination Kit	1
288	NTS2-PRO	Fluke Networks NetTool Series II	1
289	FTK1450	Fluke Networks Complete Fiber Testing Kit.	1
290	QOB130	Miniature Circuit Breaker 120V 30A	20
291	5369-C	BLK CONN-N5-20R	10
292	2311	LKG PLUG L5-20P	30
293	2613	LKG CONN L5-30R	20
294	HBL2621	LKG PLUG 30A 250V L6-30P B/W	4
295	SJOOW-10-3-BLK-250RL	Port CD 250ft roll	1
296	CAGENUT-M6-50PK	CAGENUTS	40
297	SCREW-M6-16-50PK	SCREWS	40
		NETWORKS SUBTOTAL PRICE :	
		NOSC NEST Performance Management TDC/ISO Shelter LOM	
		Enterprise Data Analysis System	
Line #	**Product Number**	**Product Description**	**Qty**
298	6980/MS	Netscout nGenius Infinistream 8-Port 4TB Probe	4
299	6980/MS SUPPMSTC	Netscout nGenius Infinistream 8-Port 4TB Probe Master Care Support	4

300	321-1582	Gigabit SX Ethernet SFP	4
		PERFORMANCE MANAGEMENT SUBTOTAL PRICE :	
		Additional Equipment Required	
		Dell OptiPlex 7010 Hardware	
Line #	**Product Number**	**Product Description**	**Qty**
301	OptiPlex 7010 Desktop Base (225-2782)	Each Dell OptiPlex 7010 Desktop Base (225-2782) - is configured per specs contained below. Each 7010 component has part numbers listed following the product description. Quantities for each part number or component are listed in the Qty Column.	130
		OptiPlex 7010 Desktop Base (225-2782)	1
		3rd Gen Intel Core i5-3470 Processor (6MB, 3.2GHz) w/HD2500 Graphics, Dell Optiplex 7010 (319-0912)	1
		4GB, NON-ECC, 1600MHZ DDR3,1DIMM,OPTI (319-0218)	1
		Dell USB KB, English, WIN7/8, OptiPlex and Precision Desktop (331-9586)	1
		No Monitor Selected, Dell OptiPlex (320-3704)	1
		1GB AMD RADEON HD 7470,LP,w/VGA,OptiPlex (320-9617)	1
		CFI,Standard Option Not Selected (365-0354)	1
		Windows 7 Professional,No Media, 32-bit, OptiPlex, English (421-5578)	1
		Windows 7 Label, OptiPlex, Fixed Precision, Vostro Desktop (330-6228)	1
		Dell Client System Update (Updates latest Dell Recommended BIOS, Drivers, Firmware and Apps),OptiPlex (421-5334)	1
		Software, DDPA (Dell Data Protection Access), version 2.3, OptiPlex x010 (421-8276)	1
		Dell MS111 USB Optical Mouse,OptiPlex and Fixed Precision (330-9458)	1
		No Out-of-Band Systems Management, Dell OptiPlex 7010 (331-6247)	1
		CFI,Standard Option Not Selected (365-0354)	1
		Heat Sink, Performance, Dell OptiPlex 7010 Desktop (331-6243)	1
		Dell AX210 Universal Serial Bus,1.2W Stereo SPKR WW,Dell Optiplex,Precision,Latitude (313-7414)	1
		OptiPlex 7010 Desktop Standard PSU (318-1892)	1
		Regulatory label, Mexico, for OptiPlex 7010 Desktop (331-7358)	1
		Enable Low Power Mode for EUP Compliance,Dell OptiPlex (330-7422)	1
		Documentation,English and French,Dell OptiPlex (331-2030)	1
		Power Cord,125V,2M,C13,Dell OptiPlex (330-1711)	1
		No ESTAR Settings, OptiPlex (331-8325)	1
		No Resource DVD for Dell Optiplex, Latitude, Precision (313-3673)	1
		Chassis Intrussion Switch,Dell OptiPlex Ultra Small Form Factor and Desktop (317-2828)	1
		1 W ready mode - exceeds FEMP 3W recommendation. Mode can be disabled in BIOS. OptiPlex (310-1959)	1
		No Quick Reference Guide,Dell OptiPlex (310-9444)	1
		Shipping Material for System,Desktop,Dell OptiPlex 990 (331-1269)	1
		No Productivity Software,Dell OptiPlex,Precision and Latitude (421-3872)	1

		OCONUS Dell Hardware Limited Warranty Plus On Site Service Extended Year (995-4403)	1
		OCONUS Dell Hardware Limited Warranty Plus On Site Service Initial Year (995-4193)	1
		OCONUS ProSupport: Next Business Day Onsite Service After Problem Diagnosis,3 Year Extended (995-2783)	1
		OCONUS ProSupport: Next Business Day Onsite Service After Problem Diagnosis,Initial Year (995-1223)	1
		OCONUS ProSupport: 7x24 HW / SW Tech Support and Assistance,3 Year Extended (995-2773)	1
		OCONUS ProSupport: 7x24 HW / SW Tech Support and Assistance,Initial Year (995-1213)	1
		Keep Your Hard Drive, 4 Year (981-3963)	1
		Intel Core i5 Desktop Sticker (331-1566)	1
		DisplayPort to DVI Adapter for Dell OptiPlex 780/990 (330-6422)	1
		Custom Operations PM Support (987-1479)	1
		Americas Merge Center Service (490-0000)	1
		Americas Merge Center, Custom Service, Fulfillment Services (490-0436)	1
		DellPlus,Information, X Image,Only (364-3626)	1
		CFI Information Swizzle, No Up,Foot,Factory Install (364-9118)	1
		CFI Routing SKU (365-0257)	1
		CFIW,Rollup,Integration Service,Hardware Install (366-1124)	1
		CFI,XImage,Fee,Integration, Factory Install (366-1289)	1
		CFI,Rollup,Integration Service,Image Load (366-1416)	2
		CFI,Rollup,Custom Project, Fee for FED (366-1550)	1
		CFI,Rollup,Integration Service,CD Image Restore (366-1558)	1
		CFI,Information,CSRouting,DIRECT,Factory Install (375-3085)	1
		CFI,Information,WIN7,VLA,ONLY,Factory Install (375-4258)	1
		CFI,Information,SC2.0,CONUS,Factory Install (375-7617)	1
		CFI,Information,MBRBR,PART,DNR,Factory Install (376-6665)	1
		CFI,Information,OPTI,7010,SD,ONLY,Factory Install (376-9177)	1
		CFI,DVD Restore,GOV,B4KJ13,Factory Install (377-1084)	1
		CFI,Image,WIN7,International,B4KJ13,Factory Install (377-1089)	1
		CFI,CBL,SATA,ODD,POWER,Factory Install (377-2544)	1
		CFI,HD,CARR,250G,ODD,REM,Factory Install (377-2717)	1
		CUSTOM ProSupport - Federal On-Site IT Support (937-5139)	1
		OptiPlex 7010 Software and Accessories	
302	(A1708251)	American Power Conversion BE750G Back UPS - 450 Watt (A1708251) **non-TAA**	130
303	(A1663779)	SCM SCR3310V2 SMART USB Card Reader (A1663779)	130
		Dell Professional P2213 22" Monitor	
Line #	**Product Number**	**Product Description**	**Qty**
304	Dell Professional P2213 22" Monitor (320-9705)	Each Dell Professional P2213 22" Monitor - is configured per specs contained below. Each monitor component has part numbers listed following the product description. Quantities for each part number or component are listed in the Qty Column.	130

		Dell Professional P2213 22" Monitor with HAS, 22.0 Inch VIS, TAA, Widescreen, VGA/DVI/DC/DP, TAA Compliant (320-9705)	1
		3YR Limited Warranty Monitor, Advanced Exchange (986-4872)	1
SC740 Cables			
Line #	**Product Number**	**Product Description**	**Qty**
305	CBL0084	CBL0084 KVM Cables - USB keyboard, mouse & dual head DVI-D video cable & audio - 6 ft.	80
306	SC740-001	SC740-xxx SwitchViewT SC 740 KVM (Keyboard, Video, Mouse) Switch - 1 user, 4 systems, SwitchView SC switch, USB, DVI-I (dual link, dual head), audio	40

APPENDIX E: RESERVED

APPENDIX F: PWS Paragraph 8.2, Estimated Government Workload

Alliant Name/Code	PWS Ref	Clearance Requirement	RFP Labor Category Name	FTE's	Annual Hours	Annual Labor Hours
Personnel elig ble for TDY's/OCONUS travel						
123G Master Information Assurance/Security Specialist	5.3.1,	TS/SCI	Senior Network/Systems Security Accreditation and Technical Writing/Documentation	1	1920	128
123G Senior/ Information Assurance/Security Specialist	5.3.2	TS/SCI	Network Security Analyst	12	23040	3072
123G Senior/ Information Assurance/Security Specialist	5.3.3	TS/SCI	Network Security	2	3840	768
123G Senior Information Assurance/Security Specialist	5.3.4	secret	Network Firewall Security	11	21120	2816
137G Master Training Specialist	5.3.5	secret	Senior Network/Systems Training and Curricular Development	2	3840	768
132G Master Subject Matter Expert	5.3.6	secret	Network Architecture Design Engineer Subject Matter Expert	2	3840	1024
133G Systems Engineer	5.3.7	secret	Enterprise Messaging Systems	10	1840	1784
126G Master Network Specialist	5.3.8	secret	Network System Design	2	3840	1024
126G Master Network Specialist	5.3.9	secret	Information Technology Systems	12	23040	4608
125G Modeling and Simulation Specialist	5.3.10	secret	Network Modeling and Simulation	3	5760	576
103G Master Applications Systems Analyst	5.3.11	Top Secret	Senior Systems Analysis	2	3840	512
123G Master Information Assurance/Security Specialist	5.3.12	Top Secret	Senior Network Security	1	1920	192
126G Master Network Specialist	5.3.13	Top Secret	Senior Network Architecture and Design	1	1920	256
126G Master Network Specialist	5.3.14	Top Secret	Senior Network Systems Design	1	1920	384
129G Senior Quality Assurance Specialist	5.3.15	secret	IT Standards Assurance	2	3840	512
129G Master Quality Assurance Specialist	5.3.16	secret	Senior IT Standards Assurance	1	1920	256
102G Senior Applications Developer	5.3.17	secret	Web-Based Application Programmer/Developer	7	12880	1016
102G Master Applications Developer	5.3.18	secret	Senior Web-Based Application Programmer/Developer	1	1920	256
133G Systems Engineer	5.3.19	secret	Network Systems Web Architect Engineer	1	1920	128
126G Master Network Specialist	5.3.20	secret	Wireless Network Architecture Design Engineer	2	3840	640
133G Systems Engineer	5.3.21	secret	Systems/Network Engineer Subject Matter Expert	4	7360	187
138G Master Voice/Data Communications Engineer	5.3.22	secret	Voice Protection Systems Engineer	6	11520	768
132G Master Subject Matter Expert	5.3.23	secret	Senior Operational Support Team Manager	1	1920	128
132G Master Subject Matter Senior	5.3.24	Secret	WAN Architecture and Design	1	1840	187
132G Master Subject Matter Senior	5.3.25	Secret	Unified Collaboration Architecture and Design Engineer	1	1840	115
114G Master	5.3.26	Secret	Senior Technical Adisor/Architect	1	1840	115
Non - Deployable personnel						
						LH/OT

101G Senior Administration/Clerical	5.2.1	Secret	**Information Technology/Knowledge Management Administrative Specialist**	2	3840	40
128G Project Manager	5.2.2	secret	**Senior Information Technology Project Manager**	1	1920	20
128G Project Manager	5.2.3	secret	**Information Technology Project Management and Logistics**	1	1920	20
135G Technical Writer	5.2.4	secret	**Information Technology Technical Writing/Documentation**	1	1920	20
133G Systems Engineer	5.2.5	secret	**Senior Systems/Network Engineer Subject Matter Expert**	1	1920	20
126G Master Network Specialist	5.2.6	secret	**Network Engineering Support**	9	17280	180
126G Master Network Specialist	5.2.7	secret	**Firewall Engineering Support**	6	11520	120
109G Senior Configuration Management Specialist	5.2.8	secret	**Network/Systems Configuration Management**	7	13440	140
109G Master Configuration Management Specialist	5.2.9	Top Secret	**Senior Network/Systems Configuration Management**	1	1920	20
125G Modeling and Simulations Specialist	5.2.10	secret	**Network/Systems Performance and Analysis**	2	3680	63
125G Modeling and Simulations Specialist	5.2.11	Top Secret	**Senior Network/Systems Performance**	1	1920	20
128G Project Manager	5.2.12	secret	**Information Technology Logistics Asset Management and Recovery**	1	1920	20
108G Computer Forensic & Intrusion Analyst	5.2.13	TS/SCI	**Cyber Intelligence Analyst/Coordinator**	1	1920	20
122G Master Help Desk Specialist	5.2.14	secret	**Senior Operations Subject Matter Expert**	1	1920	20
123G Senior Information Assurance/Security Specialist	5.2.15	Secret	**Security Analyst**	6	11520	120
122G Senior Help Desk Specialist	5.2.16	secret	**Computer Support Team**	1	1920	20
128G	5.2.17	Secret	**Information Technology Project Coordinator/Analyst**	1	1840	13
106G	5.2.18	secret	**Senior Cyber Assurance/Information Assurance Security Manager**	1	1840	50
108G Computer Forensic & Intrusion Analyst Assigned to NOSC IA, 33rd Network Warefare Sqn, Lackland AFB, San Antonio Tx	5.4.1	TS/SCI	**Network Defense and Security Analyst**	38	72960	760
106G Chief Information Security Officer Assigned to NOSC IA, 33rd Network Warefare Sqn, Lackland AFB, San Antonio Tx	5.4.2	TS/SCI	**Senior Network Defense and Security Analyst**	1	1920	20
				174		

APPENDIX G: PWS Paragraph 8.3, TDY Travel Labor Hour Estimates

PWS Reference	FTE's	TDY Labor Hours above FFP 80 hour two week pay periods.	TDY Weeks per FTE/Year
5.3.1,	1	128	4
5.3.2	12	3072	8
5.3.3	2	786	12
5.3.4	11	2816	8
5.3.5	2	768	12
5.3.6	2	1024	16
5.3.7	7	2240	10
5.3.8	2	1024	16
5.3.9	12	4608	12
5.3.10	3	576	6
5.3.11	2	512	8
5.3.12	1	192	6
5.3.13	1	256	8
5.3.14	1	384	12
5.3.15	2	512	8
5.3.16	1	256	8
5.3.17	7	1792	8
5.3.18	1	256	8
5.3.19	1	128	4
5.3.20	2	640	10
5.3.21	2	256	4
5.3.22	6	768	4
5.3.23	1	128	4
Total	**82**		